



Incident Scale & the Need for Operational Resilience

By John Contestabile & Richard Waddell



Making Schools Safe & Secure – A Local to National Effort

By Mary Filardo



Animal Relocation After Disaster – Four Cases in 2017

By Richard (Dick) Green



Podcast: Post-Disaster Relief – An Army of Volunteers

Moderated by Andrew Roszak



Preparing for a Complex Coordinated Terrorist Attack

By Deanne Criswell



Responding to the Nuclear Threat – Then & Now

By Keith Grossman



U Visas – A Hidden Homeland Security Vulnerability

By Robert C. Hutchinson



Preparedness Can Be Easy

By Raynika Battle

Our commitment to **BioDefense**
has allowed us to be ready
for the **Ebola outbreak**
in West Africa.

Now, with the **FilmArray system**
and our reliable **BioThreat Panel**,
we are able to test for 16
of the worlds deadly
biothreat pathogens
all in an hour.

Now That's Innovation!



Learn more at www.BioFireDefense.com



Business Office

P.O. Box 810
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff

Martin Masiuk
Founder & Publisher
mmasuk@domprep.com

Catherine Feinman
Editor-in-Chief
cfeinman@domprep.com

Carole Parker
Manager, Integrated Media
cparker@domprep.com

Advertisers in This Issue:

American Military University

BioFire Defense

FLIR Systems Inc.

Joint Civil & DoD CBRN Symposium

PROENGIN Inc.

© Copyright 2018, by IMR Group Inc. Reproduction of any part of this publication without express written permission is strictly prohibited.

DomPrep Journal is electronically delivered by the IMR Group Inc., P.O. Box 810, 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 Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher.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.



Featured in This Issue

Plan, Inform, Practice – Factoring in Resilience
By Catherine L. Feinman5

Incident Scale & the Need for Operational Resilience
By John Contestabile & Richard Waddell6

Making Schools Safe & Secure – A Local to National Effort
By Mary Filardo13

Animal Relocation After Disaster – Four Cases in 2017
By Richard (Dick) Green16

Podcast: Post-Disaster Relief – An Army of Volunteers
Moderated by Andrew Roszak19

Preparing for a Complex Coordinated Terrorist Attack
By Deanne Criswell20

Responding to the Nuclear Threat – Then & Now
By Keith Grossman23

U Visas – A Hidden Homeland Security Vulnerability
By Robert C. Hutchinson27

Preparedness Can Be Easy
By Raynika Battle31

Pictured on the Cover: (top row) Contestabile & Waddell, Source: ©iStock.com/artisteer; Filardo, Source: 21st Century School Fund, 2009; (second row) Green, Source: ASPCA, 2017; Roszak, Source: DomPrep, 2018; (third row) Criswell, Source: ©iStock.com/BenDC; Grossman, Source: ©iStock.com/Moussa81; (bottom row) Hutchinson, Source: ©iStock.com/welcomia; Battle, Source: Do1Thing, 2018

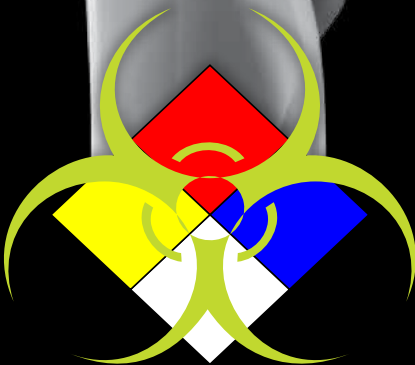
Invisible Threats Exposed



AP4C

**Portable Chemical Detection System
Protects First Responders, Military & Infrastructure**

- Fast, Reliable Analysis of Invisible Hazards Saves Time & Lives
- Unlimited Simultaneous Detection Exposes Unknown Agents
- Low Maintenance & Operation Costs Save Money
- Rugged Handheld Design is Easy-To-Use With Minimal Training
- Complete System Includes Accessories & Case for Easy Transport



[Learn More Online](#)

PROENGINE

Chemical and Biological Detection Systems

Plan, Inform, Practice – Factoring in Resilience

By Catherine L. Feinman



Modern communities are faced with myriad threats, risks, and hazards that require careful planning, significant information gathering, and actionable preparedness practices. Since incidents range in scale and scope, it is important to not only [examine the factors](#) related to the type of incident, but also examine the factors related to specific agencies and organizations. Otherwise, resilience can become a difficult goal to achieve when information needs and resource requirements are not met. The 2017 hurricane season and wildfires highlighted the interconnectedness of these factors to a community's resilience.

In addition to natural disasters, human-caused incidents can affect a community's ability to recover after a disaster – for example, terrorism, nuclear deployment, and gaps in the legal system. [Complex coordinated terrorist attacks](#), for instance, are not easily detected before an incident occurs. The [nuclear threat](#) has changed over time and requires reexamination of emergency plans, tools, and procedures. In addition, [immigration and the visa process](#) illustrate how the complexity of a process can actually create gaps and vulnerabilities.

Factors that promote resilience include the ability to protect children, relocate animals, organize volunteers, and promote personal preparedness. Investments at the local, state, and federal levels are required to protect community members and [make schools safe and secure](#) for the vulnerable populations within their walls. Coordination between jurisdictions is needed to facilitate the movement of resources into a disaster-affected area and the evacuation of the people and [relocation of animals](#) away from these areas. Management of disaster services for both large- and small-scale disasters involves [volunteer organizations](#) that fill critical resource gaps, organize response teams, and provide humanitarian services. Yet, [personal preparedness](#) remains the first line of defense when faced with emergencies and disasters. Planning for a disaster while considering numerous interconnected factors, followed by implementing the plan, are what will build and sustain a community's resilience.



Incident Scale & the Need for Operational Resilience

By John Contestabile & Richard Waddell

Numerous incidents occur every day in the United States, from simple/frequent events like automobile accidents, train derailments, and severe weather, to catastrophic/infrequent events like the 9/11 terrorist attacks, Hurricanes Harvey and Maria, and the Keystone pipeline leak to name just a few. By examining factors related to the incident and factors related to a specific entity, information needs and resource requirements can be better aligned to create operational resilience during any incident.



The number of participants and resources required to respond and recover, and the complexity of their roles and responsibilities, are significantly greater and more difficult for a catastrophic incident than for a simple incident. As complexity increases, there is a corresponding need for enhanced resilience, much of which can be achieved through increased agility. Understanding the information needs across different scale incidents provide insight into how various agencies and jurisdictions can better coordinate their resources.

Categorizing Small- to Large-Scale Incidents

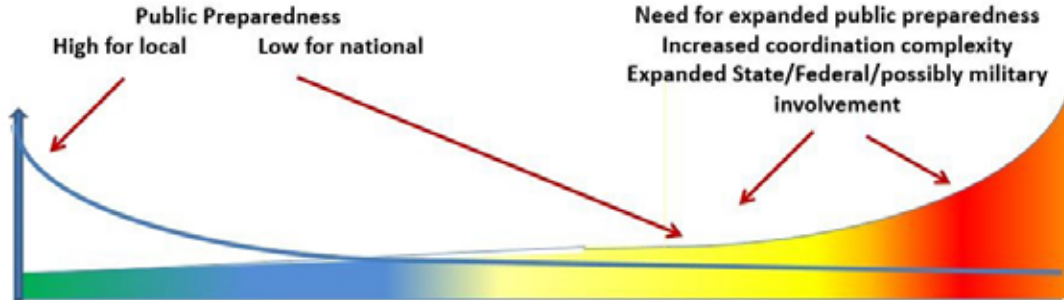
The incident-preparedness scale graphic (Figure 1) shows the interconnected nature of large-scale events. As they escalate from local to national, coordination complexity typically varies and increasing complexity emerges. The duration of an event is another significant factor. Viewing incidents at local, regional, state, and national levels recognizes that the degree of coordination required across various independent agencies and jurisdictions increases when moving from left to right (local to national). Participants must come together, coordinate, and adapt quickly as events occur, escalate, and impose cascading effects across infrastructure sectors.

The vertical scale depicts the level of public preparedness typically in place. For example, the number of first responders involved and public affected in a “local” incident is relatively small and public preparedness is high. The scene of the incident is usually cleared in less than two hours, the disruption is minimal, and there is no cascading impact on adjacent infrastructure.

However, some events rapidly grow into something more significant than initially expected. For example, a local incident may involve a vehicle transporting hazardous waste, which then spills during the event. More units and agencies would become involved and the incident scale would increase to “regional,” requiring more time to resolve (2-24 hours). During a high-traffic period, roadway congestion may cause motorists to seek alternative routes, causing “ripple effects” that could cascade to other roadways and mass transportation systems.

Some events expand into a “statewide” impact, whereas others start immediately as a state concern. The threat of a hurricane would normally start as a statewide threat, take

**INCIDENT SCALE / PUBLIC PREPAREDNESS /
INTERGOVERNMENTAL – MULTI-JURISDICTIONAL – PUBLIC INVOLVEMENT**



Classification	LOCAL	REGIONAL	STATE	NATIONAL
Examples	<ul style="list-style-type: none"> Minor traffic incidents Vehicle fires Minor train/ bus accidents Accidents w/ injuries but no fatalities 	<ul style="list-style-type: none"> Train derailment Major bus / rail transit accidents Major truck accidents Multi-vehicle crashes Hazmat spills Injuries & fatalities 	<ul style="list-style-type: none"> Train crashes Airplane crashes Hazmat incidents Multi-vehicle accidents Tunnel fires Multiple injuries & fatalities Large building fire or explosion 	<ul style="list-style-type: none"> Terrorist nuclear detonation Weaponized chemical attack Severe pandemic Strategic dirty bomb explosion Electro magnetic pulse (EMP) incident Urban bioterrorism attack Mass casualty urban explosion Major breakdown in civil order
Expected Duration	0-2 HOURS	2-24 HOURS	DAYS	MONTHS

Figure 1. Incident Public-Preparedness Scale (Source: J. Contestabile, used with permission; previously published in *CIO Leadership for Public Safety Communications: Emerging Trends and Practices*, 2012).

place over a period of days, impact overlapping local, regional, and state systems, and require activation of state and local emergency operations centers. Multiple agencies are involved as the complexity increases, requiring multiagency coordination and increased information sharing, possibly including the National Guard to supplement local and regional resources.

Finally, some events are classified as national incidents because they grow into a national disaster (e.g., disease epidemics, pandemics, wildfires, major flooding), or are so catastrophic (e.g., 9/11) that the president immediately declares them national disasters or homeland defense events. The impact of this type of event extends across multiple infrastructure sectors and touches multiple domains (air, land, sea, and cyber). Supply chain interruptions can extend for months, in geographic areas far beyond those states immediately affected. Events of this magnitude typically result in a federal disaster declaration, triggering Federal Emergency Management Agency participation, activation of the Stafford Act, and potential support from the National Guard Bureau and the U.S. Northern Command. If the disaster has a terrorism nexus, the Federal Bureau of Investigation, elements of the Department of Homeland Security, and the intelligence community would likely be involved.

Determining the Effects of Incident Scale on the Agency

Private sector companies and agencies in the public or not-for-profit sector are typically best able to manage incidents that are local in scale. These events occur most frequently, so agencies and organizations typically have considerable experience in managing the event, and the entity's resources (e.g., personnel, equipment) tend to be aligned with the challenges that incidents of this scale present. Incidents of a regional, statewide, or national scale, however, happen less frequently and have broader impact across many companies, agencies, jurisdictions, and networks such as power, water, communications, and transportation.

Although the effect of large-scale incidents can have *broader* impact, the impact on any one company or agency may not necessarily be *greater*. The actual impact to a particular entity is related to its "connectedness" to that incident. The greater the connection – either physically or virtually – the greater the likelihood is of a significant impact. A strong *physical* connection to an incident may be due to: the incident occurring on a company or agency's property or in close proximity; or reliance on a network such as power, water, communications, or transportation for its operations. A *virtual* connection to an incident may be related to: information technology or cyber assets; a contractual relationship to other entities involved in the incident; or the supply chain of which the entity is a part.

Thus, an on-premise explosion at a chemical manufacturer's plant would establish a strong physical connection to the incident; whereas, a labor strike at an out-of-state contracted partner's site would establish a virtual connection as a key supplier of material to the manufacturing process. Each would affect the entity to varying degrees.

Coping With Large-Scale Incidents

For an agency to successfully manage any incident, it must align the "tools" it has at its disposal to meet the challenges of the event. In a speech delivered by James Champy, independent consultant, author, and Harvard Business School research fellow, on 8 March 2013 at Johns Hopkins University Applied Physics Laboratory, those core tools were described as "people, processes, and technologies" (PPT). These PPTs must be integrated and aligned to accomplish basic work on a day-to-day basis. Many of these same tools are available to provide the capability to manage any incident. Thus, successfully managing large-scale incidents requires aligning PPTs to provide the requisite capability for the situation(s) presented by the incident.

It is not likely that a single entity would have every capability required to manage a large-scale incident because of funding constraints. Some needed resources may lie outside the entity's control. For example, a company that transports chemicals would likely be prepared to respond to a small, localized, on-premise spill of a few gallons. But for an off-premise spill of several hundred gallons into a stream, contracted resources would likely be needed and external agencies notified. If the spill involves hazardous chemicals, evacuation may be required; this is usually the responsibility of fire or law enforcement agencies, which are likewise outside the company's control.

To enhance resilience, a facility must determine what capabilities are needed to plan for, respond to, and recover from incidents beyond localized events and how much to invest in such preparedness, given the relatively infrequent nature of these large-scale incidents. This

determination can only be made after assessing the relative risks, the likelihood of various large-scale scenarios occurring, and the possible impact(s).

In addition to having the capability to manage an incident, responders must be able to apply and adjust those capabilities in a rapidly evolving situation. The dynamic nature of unfolding incidents requires a certain organizational agility to be effective. Although agencies and organizations try to anticipate likely emergency events and plan accordingly, the reality is that every event is different in some respects from the scenarios used for planning. As such, flexibility and agility are needed to respond successfully. [Agility in this sense](#) incorporates the ideas of flexibility, balance, adaptability, and necessary coordination.

Agility is in large measure dependent on awareness of the incident. That is, operators must first discern that an incident has occurred and then have ongoing, accurate, awareness of unfolding or cascading events to take appropriate action. These are necessary conditions to remain effective as the incident changes over time – from response to recovery phases.

Defining Critical Success Factors for Large-Scale Incidents

Although many factors influence resilience as incident scale increases, a few factors have been identified thus far. It may be useful to think of this matter as a “ledger” whereby certain factors are associated with the incident on the one side and factors associated with the agency on the other (see Table 1). The incident factors are stressors affecting the entity, whereas the entity factors are useful coping mechanisms. Using the terms and factors in Table 1, lists parameters that define the incident as well as the tools the agency has to address the challenges presented by the incident.

Table 1. Factors Influencing Resilience as Incident Scale Increases

Incident-Related Factors	Entity-Related Factors
Scale: <ul style="list-style-type: none"> • Local • Regional • State • National 	Capabilities: <ul style="list-style-type: none"> • People • Processes • Technology
Connectedness: <ul style="list-style-type: none"> • Physical – proximity to and dependence on power, communications, water, transportation • Virtual – cyber, contractual, supply chain 	Awareness: <ul style="list-style-type: none"> • Initial • Ongoing
	Agility: <ul style="list-style-type: none"> • Flexibility • Balance • Adaptability • Coordination

Following are some questions to consider for *incident-related* factors:

- What scenarios does the entity want to prepare for?
- What are the various types of events experienced in the past?
- Are the designed scenarios sufficiently challenging? Would they likely challenge the whole agency?

- Has the entity considered a “worst case” scenario? Have it exercised “out of the box” thinking?
- How will the entity know an incident has occurred? Will this awareness remain if normal communications are disrupted?
- How connected is the entity to each scenario?
- Are there scenarios that occur both on premise as well as off premise?
- Can the entity discern impacts from the off-premise scenario (as these may not be obvious)?
- Considering each of the critical external inputs of power, communication, water, and transportation, how does the disruption of each affect the entity?
- What are the supply chain impacts of each scenario? Are there unintended effects/consequences that will affect the entity? How will the entity know?
- How/when will contracted resources be accessed? What guarantees are there that the resource will be available?

Following are some questions to consider for *entity-related* factors:

- Does the entity have the requisite staff with the necessary skills to manage this scenario? Will they be available when needed?
- How will staff be contacted/activated during this scenario? Is there a policy/protocol/concept of operations addressing this?
- Do staff members have the requisite training and equipment to manage this scenario?
- What provisions have been made for the families of key staff?
- How/when will management be notified in this scenario? What methods will be used? Are there alternative methods should the usual be unavailable?
- Are there “workarounds” for a loss of the external inputs of power, water, transportation, and communication?
- Can the entity still function (albeit at a reduced state) in the face of the loss of these inputs? If not, does the entity “fail gracefully”? What steps must be taken to “shut down” the entity? Conversely, what steps must be taken to “start up” the entity?
- What are the trigger points at which the entity must make key decisions? Are there values/measures of performance for those triggers that can be utilized in a concept of operations? Is there a technological tool utilized?
- Does the scenario create vulnerability in the entity’s cyber posture? How will systems continue to operate with potential staff shortages and reduced power? Are certain IT staff designated as “key” and required to report?
- How will management remain aware of the current situation during the course of the scenario? During the recovery phase? Is there a technological tool utilized?

- What is the plan for releasing information to employees? To the public? Is social media involved in that process?
- With what external stakeholders – for example, fire, police, emergency management, suppliers, customers – must the entity coordinate? When? By what methods?
- When does the entity determine the need for mutual aid? Who makes that decision? What is the process for doing so? How would it be done with reduced communications capability?

Consideration of the above scenarios and questions should reveal the entity's shortcomings, which include but are not limited to the following:

- Lack of policies and procedures
- Incomplete concept of operations
- Lack of staff with the requisite skills
- Lack of training and exercising
- Contractual shortfalls
- Communications gaps
- Technological issues
- Notification/coordination gaps
- Supply chain vulnerabilities
- Cybersecurity issues
- Lack of situational awareness
- Areas of limited flexibility

Incident scale refers to the incident's breadth of impact, but an entity's connectedness – both physical and virtual – will determine that entity's resilience.

For each of the above, a corrective action plan can be developed to strengthen the entity's posture and increase its resilience. Through effective oversight and governance, additional remedies can be implemented to improve preparedness, response, and recovery activities.

Recommendations

Two recommendations for improving operational resilience were provided by Rogier Woltjer et al. in their presentation, "An Overview of Agility and Resilience," at the Resilience Engineering Symposium, 22-25 June 2015, Lisbon, Portugal:

First, *understand the nature of the incident* for which to be prepared. Typically, the focus would be on regional/statewide/national events as, presumably, sufficient capabilities already exist to manage local events. Gaining this understanding would involve scenario exploration and an examination of that entity's incident response history. It also requires some consideration of worst-case scenarios. In each scenario, understand the connectedness of the agency to the incident. Examine physical and virtual connections and dependencies.

Second, *understand the nature of the entity's capabilities* to plan for, mitigate, respond to, and recover from the identified scenarios. This would include how the agency would become aware that an incident may have occurred. It would also involve an examination of various business processes and technological systems as well as staff skill sets that could/should be

brought to bear. Also, understand the entity’s ability to be agile, which includes the capability to provide notifications, establish and work within incident command structures, mobilize resources, and call for mutual aid.

Certainly, there is much to be researched and learned to understand just what it means to be “resilient.”

This article is based in part on the Resilience Engineering Association’s ongoing body of work, which was originally inspired by “[Resilience Engineering: Concepts and Precepts](#),” by Eric Hollnagel, David Woods, and Nancy Leveson in 2006. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position of the Johns Hopkins University–Applied Physics Lab.

John Contestabile (pictured above) is the program manager for emergency response systems for the Johns Hopkins University/Applied Physics Lab. He joined the Lab in July 2009, after retiring from the State of Maryland Department of Transportation (MDOT), where he was acting assistant secretary for administration responsible for, among others, emergency management and homeland security. In addition, he was named acting deputy homeland security advisor by Governor Robert Ehrlich and later the director of the Maryland State Communications Interoperability Program (MSCIP), reporting to the superintendent of the Maryland State Police, by Governor Martin O’Malley. He is also a member of the Preparedness Leadership Council International.

Richard “DJ” Waddell is a principal staff systems analyst at the Johns Hopkins University Applied Physics Laboratory. He has extensive experience developing and managing technology solutions and is currently focusing on homeland protection projects on the technology needs of state and local first responders and emergency managers. He is the founding director of the National Criminal Justice Technology Research, Test and Evaluation Center. The Center is funded by the Office of Justice Programs, National Institute of Justice, under Award #2013-MU-CX-K111.

Joint Civil & DoD CBRN Symposium

March 5-6, 2018 | Alexandria, VA



Advancing a Government Wide Approach to CBRN Defense, Readiness, and Response

JOINTCBRN.DSIGROUP.ORG

Making Schools Safe & Secure – A Local to National Effort

By Mary Filardo

This article explores the meaning of safe and secure schools, shows where current schools are falling short, and offers policy prescriptions, pointing to the pending federal infrastructure package as a unique opportunity to make an important down payment to secure a safer and better future for the nation's students.



Each day, one in six Americans – over 50 million students, teachers, and other adults – enter public schools. Despite having a right to be safe and secure from a variety of threats, not all school buildings and grounds provide the level of safety, security, and educational functionality that meet modern industry facilities spending standards (see page 21 of the 2016 “[State of Our Schools: America’s K-12 Facilities](#)”). Next to highways, public school facilities are the nation’s [second largest infrastructure investment](#) at the state and local levels. In 2013, the [average school was 44 years old and 53% were estimated to need repairs, renovations, and modernization](#) to put them in good overall condition. Low-wealth urban and rural communities are especially affected by substandard buildings. State and local control of facilities can be preserved and community efforts leveraged with federal funding for public school infrastructure. A local, state, and federal partnership is needed to ensure all students are in safe and secure facilities when attending public school.

Public school districts strive to facilitate learning and knowledge in a safe and healthy environment, so students can flourish in both mind and body. School districts have a responsibility for the health, safety, and security of children while they are in their care – legally referred to acting *en loco parentis* – in place of the parent. However, with aging schools and a structural gap between the financial budgets required to provide modern schools and what school districts and states have been able to do alone, many schools have been falling short.

Healthy Schools

Without increased capital investments in the built environment, school districts will not be able to meet modern standards for healthy, safe, and secure school facilities. Hazardous building materials from an earlier age linger, such as asbestos, lead, and polychlorinated biphenyls ([PCBs](#)). These legacy chemicals actively harm students’ health, and are linked to asthma as well as liver, lung, and kidney damage. These toxins, particularly lead, affect young children, stunting brain and neural system growth. The effects from these toxic materials are increased when the facility is deteriorated – a leaky roof causes lead paint to peel off ceilings and walls, for example.

Safe Schools

As the place where millions of children go each day, public schools are being called on to meet stricter codes to protect children and communities during times of natural disaster. During hurricanes, tornadoes, floods, mudslides, or wildfires, school facilities must protect



Addition on a 1960s public school, being modernized in 2009 (Source: 21st Century School Fund, 2009).

children and adults in the school, but also must operate as a shelter for those who are displaced, and as essential command and control centers for local response teams, as well as aid distribution centers for the community. Even so, many schools are not designed, built, or modernized to incorporate new building practices and materials that make school buildings more resilient. In aging school facilities, even safety essentials – like working fire alarms, appropriate egress hardware, and highly fire-rated safe-areas – are not universally in place.

Secure Schools

Schools must not only be healthy and safe places, but they must be secure for students, teachers, and other staff. In districts where high crime rates have plagued communities, many high schools have installed [metal detectors](#) and hired [school resource officers](#) to facilitate a secure environment. But what used to be targeted security concerns have expanded due to devastating school shootings – Columbine High School in 1999, and Sandy Hook Elementary School in 2012. The increased access to high-powered firearms made these incidents more devastating and dramatically amplified the loss of life. These tragedies, and others, have increased the desire of communities to build security into their school design. Both Homeland Security’s framework for resilience – touted in the most recent National Incident Management System (NIMS) document, released in October 2017 – and Crime Prevention Through Environmental Design (CPTED) emphasize a comprehensive approach to public security that can apply to public schools. However, generally, school facilities security improvements are often ad hoc and after the fact.

States & Districts – Doing Their Share

According to the “State of Our Schools: America’s K–12 Facilities” report, the nation’s public school districts, with help from most states, spent an annual [average of \\$49 billion per year](#) (at 2014 values) on public school construction during the fiscal years from 1994 to 2013. Almost half of local funds were for new schools, as elementary and secondary public school enrollment increased by nearly 10 million students beginning in 1990. The nation’s budget-constrained school districts held [\\$425 billion in long-term debt nationwide](#) a state average of \$7,448 per student – at the end of FY2015. Local school districts have historically provided the majority of funds to build school facilities – [approximately 82% with state governments providing the other 18%](#). That said, 12 states provide no aid for capital construction responsibilities.

In addition, according to the “State of Our Schools” report, “although the federal government contributes about 10% to annual operating budgets, it provides almost no support for capital construction.” Only once schools have already been damaged or destroyed by natural disasters is federal funding for such expenses provided through the Federal Emergency Management Agency.

Emerging Federal Efforts

There is a growing [effort to secure federal support](#) to supplement, not supplant the local and state responsibilities for modern, safe, and secure public school facilities. The reason is clear. School districts have a critical gap between funding and needs, which the “State of Our Schools” report projects will increase at a rate of \$38 billion each year over the next 10 years, severely limiting the ability of school districts to provide a healthy, safe, and secure environment for students and staff.

The case for additional capital investment in schools and a fair federal share has gained traction recently in Congress and the Executive Branch. Congressman Bobby Scott (D-Virginia) and Senator Jack Reed (D-Rhode Island) have both introduced bills addressing funding gaps. Their proposed legislation would allocate \$100 billion for school facilities modernization over the next 10 years. Such investments will not only make facilities more secure for the long term, they will catalyze jobs and local economic growth in the short term. As of mid-January 2018, the Scott bill ([H.R.2475](#)) had 109 cosponsors and the Reed bill ([S.1674](#)) had 14.

In addition to the two bills in Congress, the Trump Administration – with the completion of tax reform – has pivoted toward another major campaign promise, infrastructure. President Donald Trump campaigned on the promise of creating a [\\$1 trillion dollar infrastructure package](#) and included schools in his speeches about infrastructure before and after the election. The administration’s infrastructure package represents a unique opportunity for school facilities to receive the critical funding needed to help make schools safer and more secure.

A one-time, single infusion of federal dollars into the neediest school districts would not create a cycle of dependency for local school districts, but rather would help close a critical gap that has long created inequitable conditions in thousands of schools. Safe and secure schools positively influence student learning as well as student, teacher, and staff health. State and local governments are doing all they can do. It is time for the federal government to step up. Healthy, safe, and secure public school infrastructure is basic. It is an essential requirement for the nation’s health, safety, security, and prosperity. To learn more, visit www.buildusschools.org

Mary Filardo, executive director of 21st Century School Fund, founded the 21st Century School Fund in 1994 to improve the policy and practice of planning, design, construction, management, and financing for the District of Columbia public schools. In 2001, with support from the Ford Foundation, she started Building Educational Success Together (BEST) to work nationally on these issues. She has written extensively on public school facilities, developed software to support public engagement in facilities master planning, and piloted public-private school development partnerships. She holds a BA in philosophy and mathematics from St. John’s College, and a MPP from the University of Maryland. She was the 1979 Truman Scholar from the District of Columbia.

Animal Relocation After Disaster – Four Cases in 2017

By Richard (Dick) Green

Between late August and the end of 2017, the American Society for the Prevention of Cruelty to Animals (ASPCA) deployed to six states and the U.S. Virgin Islands in response to four disasters: Hurricanes Harvey, Irma, and Maria, and the wildfires in Northern California. In all, the ASPCA assisted nearly 37,000 animals affected by these disasters. Although each response required a unique approach, one particular objective was consistent throughout, which likely saved thousands of animal lives – animal relocation.



Local government typically imposes a minimum holding time for animals that are brought into a community shelter. After their holding time is complete, these animals are available for adoption. When a disaster is imminent, shelters try to move these unclaimed animals out of the shelter to ensure their safety and to make room in case more animals arrive after the disaster strikes. This process of moving unclaimed animals is referred to as “relocation” or “relo.”

The goal in a relocation effort is to place the at-risk animals in parts of the country where there is the greatest likelihood for finding new homes. The ASPCA has a large network of receiving shelters for this purpose. In 2017, the ASPCA Animal Relocation team helped transport more than 1,600 homeless animals out of communities struck by disasters. Many of those animals have already been adopted.

Hurricane Harvey

When there is over 40’ of rain – and in some places over 50’ – stranded humans and animals are likely. Hurricane Harvey provided just that scenario, with [122,331 people rescued or evacuated](#). A rule of thumb in animal emergency response is that pet population ranges between 52% and 59% of the human population. This suggests that thousands of animals were rescued following Harvey in August 2017. In anticipation of Harvey’s landfall in Texas, a number of animal shelters began to transport shelter-owned (unclaimed) animals out of state. Relocation activities started several days before landfall and continued for several weeks after the storm. The Texas Animal Health Commission estimated that 765 companion animals were in state-run co-located shelters and 1,424 pets were in independent shelters. Many animals that were not reunited with their owners were transported to neighboring shelters.

The ASPCA’s search-and-rescue and medical teams deployed to multiple locations in both Texas and Louisiana following Harvey’s landfall and assisted or established emergency shelters for displaced animals in Dallas and Sour Lake, Texas. There, hundreds of owned pets were cared for until their owners could return home to claim them. In addition, the ASPCA evacuated hundreds of animals from Texas – some of whom were relocated to the ASPCA’s Adoption Center in New York City.

Hurricane Irma

Similar to Hurricane Harvey, relocation efforts played a critical role before and after Irma made landfall in September 2017. Given the general agreement on the tracking of the storm – and with memories of Matthew fresh on residents’ minds – evacuations were underway well before Irma even hit Cuba. Animal shelters in Florida, Georgia, and South Carolina were seeking assistance in moving their unclaimed animals out of state. It is important to note that shelters in the south move pets to areas in the north all year long and many shelters have established partners that are willing to take their unclaimed pets and, in some cases, are even willing to come pick them up.

In a disaster, with limited resources, a rescue group cannot afford to take a transport vehicle out of service for any length of time. In the case of Irma, the ASPCA set up a waystation in Duncan, South Carolina. This 40,000 square-foot emergency shelter temporarily housed evacuated animals from three states and scores of agencies. Nearly 600 animals were sheltered there until the Animal Relocation team identified receiving shelters. In total, the ASPCA assisted more than 11,000 animal victims of Hurricane Irma through water and field search-and-rescue operations, emergency sheltering, distribution of pet food and supplies, and relocation efforts.

Hurricane Maria

On the mainland, it is relatively easy for a family to evacuate with pets, assuming plans were made early and transportation is available. However, living on an island is more challenging for evacuating with pets. Seats are limited, airlines have become more restrictive on how pets fly, and it is expensive. Consequently, a much smaller percent of residents evacuate from an island with their pets than do their counterparts on the mainland. In the case of Hurricane Maria hitting Puerto Rico and the Virgin Islands in September 2017, hundreds – if not thousands – of animals were displaced, abandoned, or free-roaming.

At the request of the Federal Emergency Management Agency (FEMA) and the Virgin Islands Department of Agriculture, the ASPCA deployed its disaster response team to St. Croix to help assess needs for animals affected by the Category 5 storm and establish an emergency shelter for displaced animals. For more than three months, nearly 150 responders were deployed to perform animal search and rescue and to provide daily care for small and large animals. Veterinary and behavior experts provided ongoing support for nearly 600 displaced animals at the ASPCA emergency shelter. Every animal that the ASPCA took in was reunited with their families, adopted to new families, or transported off the island.



After Hurricane Maria, two dogs tangled under a mangled fence while responders work to rescue them (Source: ASPCA, 2017).

Although transporting an animal by air is faster, it is not as cost-effective as by land. For example, an air transport of 100 animals could easily cost up to \$50,000. In Puerto Rico and the Virgin Islands, it was difficult to get in larger airplanes, which meant that multiple trips were needed using smaller planes with a capacity of 30+ animals. Nearly 400 cats and dogs – either not owned before Hurricane Maria or surrendered afterward – were relocated from St. Croix to the ASPCA's expansive network of shelters and rescue groups on the mainland United States, where they were made available for adoption. According to the Humane Society of the United States, [over 2,000 animals](#) were airlifted from Puerto Rico.

California Wildfires

The first request the ASPCA received for the northern California fires in October 2017 was to provide emergency sheltering supplies for Mendocino and Sonoma counties. With the assistance of the American Red Cross and American Logistics Aid Network, the ASPCA was able to transfer supplies from its warehouse in San Francisco to affected areas within 24 hours. The Tubbs Fire, which was the largest and most destructive of the complex of fires, hit Sonoma County and the Napa Valley quickly and late at night – providing very little warning and little time for people to evacuate with their pets. Livestock and specifically horses were at the greatest risk as owners rushed to transport their animals to the Sonoma County Fairgrounds. At one point, over 700 horses were at the fairgrounds and hundreds of pets were sheltered in co-located and co-habitated shelters throughout the county.

[It is estimated](#) that over 5% of available housing in Santa Rosa was lost to the fire, making it very difficult for residents to find adequate housing for themselves and their pets. Consequently, a significant number of pets have either been relinquished or boarded with facilities outside the county. Since this put a significant burden on bay area shelters, requests were issued for help in relocating unclaimed animals to make room for fire victims. With the cooperation of Alaska Airlines, more than 30 cats and dogs were moved from the bay area to ASPCA partners in the region.

In 2017, the ASPCA was active in 19 states with 30 deployments, rescuing 4,500 animals and assisting 40,000 animals through search and rescue, sheltering, and relocation program.

Richard (Dick) Green, Ed.D., is the senior director of disaster response for the American Society for the Prevention of Cruelty to Animals (ASPCA). Before the ASPCA, he was the emergency relief manager for disasters at the International Fund for Animal Welfare (IFAW). He has responded to international and national disasters, and his teams have rescued thousands of animals from floods, tornadoes, fires, and hurricanes. Recent international responses include typhoons in Taiwan, Philippines, and Australia, volcano eruptions in Philippines and Iceland, and earthquakes in China, Haiti, and Japan. He has trained hundreds of responders in disaster prevention and response and has developed training curricula and texts for Slackwater Rescue, Water Rescue for Companion Animals, and Rope Rescue for Companion Animals. He is the past chair of the National Animal Rescue and Sheltering Coalition, is on the Board of Directors for the National Alliance of State Animal and Agricultural Emergency Programs, co-chairs the Animal Search and Rescue Best Practice Working Group, and is a member of the Evacuation and Transportation Best Practice Working Group. His doctorate is in education with an emphasis in kinesiology and biomechanics. He was an educator for 27 years, the last 10 at Gonzaga University in the Department of Exercise Science.

Post-Disaster Relief – An Army of Volunteers

Launched by Methodist minister William Booth and the East London Christian Mission in 1865, The Salvation Army provides services during both daily operations and times of disaster. More than just thrift stores and bell ringers, The Salvation Army provides small- and large-scale disaster relief – from house fires to major hurricanes. This “Army of Good” includes about 5,000 officers, 60,000 employees, and more than 1 million volunteers located in 26 countries and across the United States.

Following a disaster, The Salvation Army sends teams to evaluate the scope of the disaster, to develop a response plan, to request donations, and to work with governmental and other nongovernmental organizations to provide victim relief, feeding kitchens, and pastoral duties. Volunteer organizations are critical assets for disaster response, yet back-to-back disasters like the hurricanes and wildfires experienced in 2017 raise concern about donor and responder fatigue. Listen to this podcast and visit www.salvationarmyusa.org to learn more about this organization and its capabilities – a critical resource for all those responding to and affected by a disaster.

[Click](#) to listen.

Andrew Roszak, Moderator, Senior Director for Emergency Preparedness, Child Care Aware® of America

Lt. Colonel Ward Matthews, The Salvation Army USA National Spokesperson and Community Relations and Development Secretary

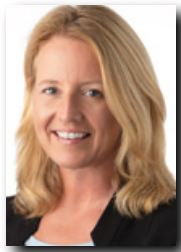
Lt. Colonel Michele Matthews, The Salvation Army USA National Director for White House Relations



Preparing for a Complex Coordinated Terrorist Attack

By Deanne Criswell

Complex coordinated terrorist attacks (CCTAs) are exactly as the name implies: large-scale attacks that are multifaceted, well-planned, and often involve multiple perpetrators. These individuals are often unknown to law enforcement, making them difficult to identify during pre-operational planning activities. Because of their size and complexity, these types of attacks far too often have a devastating impact across jurisdictions, disciplines, and even state lines.



Needless to say, responding to a CCTA attack is highly complex, creates confusion, and is difficult to know what will happen next. Preparation begins with the local patrol officer and must expand to include the whole community. The best way to prepare for, and respond to, a CCTA is to think outside the proverbial box – as well as outside the lines of traditional jurisdictions, disciplines, and states. CCTAs require a whole community response, with decision-making before, during, and after this type of event being a collective effort. Coordination is paramount.

Simply knowing where to start can be a challenge for communities to establish coordination and create a collective response. Challenges can also occur when working across disciplines and jurisdictions – particularly when each is “in charge” of its own community and operations. To help with the preparedness process, the steps are mapped, challenges identified, and solutions provided to aid emergency managers in creating the community response necessary for an effective CCTA response plan.

Step 1: Bring the Community Together

One of the first, and most important, steps is to bring the whole community together. CCTA preparedness activities must be tailored to each jurisdiction and account for complex and evolving terrorist tactics, techniques, and procedures. The solution will not be found by utilizing a government-centric approach. It will require coordination from the entire community. Start by contacting established relationships – those who are already involved. Then include stakeholders from other jurisdictions and disciplines, as well as law enforcement, hospitals, and firefighters. Define the role that each stakeholder plays and determine the resources that each organization could provide.

After establishing the baseline, think about what might be missing. For example, consider including nonprofits such as the Red Cross, government agencies, local military installations, and community stakeholders outside the emergency management community, such as academia and the private sector. This is a lot of people to invite to the planning table. However, through this approach, everyone who may have even the smallest role is invited to participate. The result is a collaborative planning process that gains stakeholder buy-in, fosters new relationships, and encourages open communication.

Step 2: Identify Gaps

Once everyone is at the table, the next step is to conduct a gap analysis to identify: what is missing; strengths and weaknesses of the entire plan (in training, exercising, and personnel); and any skill-set short falls. Because most jurisdictions have not experienced a CCTA event, it is imperative that there is also a review of past events – after action reviews, best practices, and/or capabilities – and how they might apply to a specific jurisdiction. This is also a good

time to identify policy gaps, such as mutual aid agreement and communications plans. One of the greatest challenges in cooperation across jurisdictions and disciplines is successful communication. Each group has its own well-established methodologies, yet a joint effort requires agreement on a single solution that may be different than some groups are accustomed to. Discuss topics such as communication protocols, communication frequencies, back-up communication methodologies, and who will take the lead on communications efforts.

Step 3: Plan How to Work Together

With a room full of leaders, it may be challenging to determine who will have which responsibilities – that is, developing an understanding of how a multidisciplinary, multijurisdictional response will come together. When planning for a CCTA at the Office of Emergency Management for the City of Aurora, Colorado, a core group of stakeholders from multiple disciplines actively discussed the pros and cons of different response scenarios. The group discussed how to move forward in each scenario, who was trained for which types of event, and the best solutions.

For example, the group determined that, in an active shooter scenario, the best course of action would be to have the paramedics enter with the SWAT team to neutralize the threat while treating potential victims. Different scenarios saw different approaches based on training and skillsets. Every jurisdiction has unique needs; therefore, multiple scenarios should be planned with the understanding that different events may require different approaches. The more conversation and planning, the better.

Step 4: Train & Exercise

Planning and reality are dramatically different. Although planning can occur years in advance, reality almost never mimics that plan. The best way to truly understand preparedness levels for a CCTA is to train and exercise – specifically, cross-disciplinary training:

- Train to multiple scenarios. Even the most outlandish scenarios can become real, and the more outlandish, the greater the threat. Plan for the unexpected.
- Train across disciplines and jurisdictions. The goal is to use cross-discipline and cross-jurisdictional resources to thwart a potential CCTA. The only way to know if a plan will be successful is to conduct trainings using all the resources involved in the plan. Training piecemeal does not work.
- Most importantly, train to failure. As a former colleague from the City of Aurora would often say, “a training exercise that goes perfectly had a really bad design.”

Although communities hope never to experience a CCTA, they should all be prepared for the possibility in a way that is specific to a CCTA-type of incident. A complex, coordinated incident requires an equally complex, coordinated response. It requires the whole community; it requires careful attention to potential pitfalls or gaps in the plan; and it requires training and exercises that go beyond the routine and scale to the size of a potential large, complex, coordinated incident.

Deanne Criswell has more than 25 years of emergency management experience, including federal, military, and local government response to complex incidents and disasters. She served as the leader of one of the Federal Emergency Management Agency's (FEMA's) National Incident Management Assistance Teams (N-IMAT). She also served in the National Guard, and was the manager of the Office of Emergency Management for the City of Aurora, Colorado, where she led strategic change in the city's emergency and disaster planning. She currently serves as principal in the homeland security sector for Cadmus. She is a certified emergency manager by the International Association of Emergency Managers.

EMERGENCY SERVICES WEBINAR SERIES 2017

KNOWLEDGE WHEN YOU NEED TO RESPOND

In the world of emergency operations, conditions change. So does the knowledge needed to respond effectively. American Military University (AMU) is proud to host a series of free, 1-hour webinars for responders and emergency managers, covering these and other essential topics:

- Violent Incident Consequence Management, the Emergency Manager's Role
- Principal Investigator for the Firefighter Injury Research and Safety Trends (FIRST)
- Drafting and Implementing Effective Fire Department Policies and Procedures
 - Financial Systems Management for Fire and EMS Agencies
 - Organized Response to Mass Casualty
 - Firefighter Health: Heart Healthy Solutions

Webinar attendees may receive a 5% tuition grant for degree and certificate courses at AMU.

REGISTER FOR THE WEBINAR SERIES TODAY AT
PUBLICSAFETYATAMU.COM/DPJ

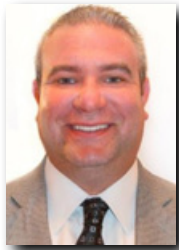
FOR MORE INFORMATION ABOUT CUSTOMIZED
TRAINING TO MEET YOUR NEEDS, CONTACT ANTHONY MANGERI AT
AMANGERI@APUS.EDU.



Responding to the Nuclear Threat – Then & Now

By Keith Grossman

In the civil defense era of emergency management, the federal, state, and local civil defense authorities were presented with the mission to protect the civilian population from an attack on the U.S. mainland. Shelter programs, coordinated public warning systems, emergency assistance provisions, and other protective measures were developed. Today, these measures need to be revisited and adapted in accord with current threats, timing, and resources.



The Office of Civil Defense and Mobilization was created by President John F. Kennedy via [Executive Order 10952](#) in September 1961. This executive order established the creation of the [Community Fallout Shelter Program](#), developed a coordinated public warning system, employed the provision of emergency assistance to state and local governments, and empowered the Secretary of Defense to plan for the continuity of government. It is important to put this in the context in which this executive order was enacted. These programs and initiatives occurred during the Cold War, in the atomic age, with a growing nuclear threat from Russia, and growing concerns from U.S. citizens over the effects of a first strike.

The United States is now faced with a renewed conversation about a nuclear threat, causing Hawaii to activate and perform a monthly test of their [State Attack Warning Tone](#) for the first time since the Cold War. The most recent routine test of the system created a widely publicized [false alarm](#) that occurred at 8:07 am on 13 January 2018 (see Fig. 1). This false alarm highlighted a flaw in Hawaii's warning system in which a singular person could initiate activation. Hawaii is now moving to a two-person activation method in the aftermath of this event. Given the time lapse since the Community Fallout Shelter Program was established in 1961, [many fallout shelters have since been closed](#), this poses the question of what would happen should this alarm have been real.

Historical Review

In order to fully understand the current situation, it is important to understand the origins of civil defense. President Franklin Delano Roosevelt established the Office of Civilian Defense ([OCD](#)) in 1941 to plan for a community-based response to protect civilians in the event of a military attack



Fig. 1. Emergency alert received by residents in Hawaii was a false alarm (Source: @TulsiGabbard, 2018).

on U.S. soil. The OCD was an independent agency that coordinated with the Chemical Corps of the U.S. Army and the U.S. Public Health Service. When it was created, this office looked at the many hazards with which a community would be presented after a land attack.

At the end of World War II, the office was disbanded due to the decreased threat. This changed over the course of the next decade as the world entered the atomic age following the bombing of Hiroshima and Nagasaki in Japan and Russia detonating its first atomic weapon. As atomic threat became reality, the OCD went through several iterations throughout the years, most notably as the [Federal Civil Defense Administration](#) under President Harry S. Truman in 1951 and the Office of Civil Defense and Mobilization beginning in September 1961.

With the creation of the Community Fallout Shelter Program, thousands of shelters were built across the United States, especially in urban centers. The program focused on creating infrastructure and capacity along with a stringent training and exercise program. For many, the memory of a fallout shelter and “[Duck and Cover](#)” drills during elementary school remain. Throughout the decade-long tenure of this program, countless home and public shelters were

built throughout the country, creating a sense of security and a belief that people could easily survive nuclear fallout in their geographic areas.

Much can be learned from the principles of the civil defense era, especially as the nation now faces a renewed conversation about nuclear threats.

A significant amount of research was also performed on the human condition during an extended stay in a shelter with only Department of Defense rations, chemical communal toilet canisters, poor ventilation, and

overcrowding. It was found that a lack of sleep, the chemical commode, and a lack of bathing facilities caused major discomfort, as well as headaches and nausea. Additional psychological issues included the ability to adjust to hygiene and decontamination rituals, to adapt to the change in living conditions, and to adapt to the uncertainty that lay outside. The response to these issues was training and the creation of motivational in-shelter programs that would enable people to emerge from the shelter in an emotionally stable condition. To a great degree, the activities may not have been realistic but designed to stabilize and support the anxiety and concerns exhibited by the populace.

For example, the OCD created a guidance document, entitled [Fallout Protection](#). This training aid was used to guide families and communities in their preparedness and planning for a nuclear attack. It instructed families to stay in their fallout shelters for at least 14 days, and come out in increasing intervals beginning at no more than four hours per day. The Fallout Protection guide not only gave information regarding the effects of a nuclear blast and the subsequent fallout, but also gave instruction on supplies needed for survival. Additionally, this era led to the build out of multiple sites for continuity of government including: Orange One, which is the president’s bunker at Camp David; and Site R (Raven Rock Mountain Complex), which is the emergency operations center for the U.S. military.

In 1969, Congress began defunding the Community Fallout Shelter Program and, by 1972, merged the Office of Civil Defense and Mobilization into the [Defense Civil Preparedness Agency](#). Since many of the public shelters were reliant on federal funding to maintain their functionality, the lack of funds diminished the feasibility of the shelters. In 1979, President James “Jimmy” Carter issued [Executive Order 12148](#), which dismantled the Defense Civil Preparedness Agency and transferred all of its responsibilities to the Federal Emergency Management Agency. Since that time, the national response has moved away from a nuclear focus, and toward the all hazards approach currently used as the industry standard.

Changes & Current Standards

The primary change has been related to timing. In the 1960s, a nuclear device was delivered by plane, with an advanced warning potentially of up to 40 hours. In the age of the intercontinental ballistic missile (ICBM), notice is significantly shorter, usually less than one hour of lead-time. This is not enough time to report to an assigned community fallout shelter. As such, the focus has shifted to surviving the blast and staying indoors in the most central part of the nearest building when the blast occurs.

In addition to the launch of an ICBM, threat of a dirty bomb release exists and can happen with virtually no warning. In the case of a dirty bomb, the actual blast would likely not be the most deadly part of the attack. The fallout created by the release could create long-lasting health and safety issues in the region where the attack occurred.

Although there is a marked change in the timing of a release, the fallout risk remains the same in the aftermath of the event. In present day Hawaii, emergency planners have re-tooled some of the Civil Defense Era planning and response methods. As previously mentioned, the state of Hawaii has resumed testing of the state attack warning tone. It has also reissued a [Guidance Summary for Coordinated Public Messaging on Response to a Nuclear Detonation](#). This document gives similar advice as its predecessor, the Fallout Protection pamphlet issued in 1961. It advises people to get inside immediately, stay away from windows, stay low to the ground, stay inside for up to 14 days, and venture outside only to find essential supplies. The major difference between these two guiding documents is simply the lack of need for or use of fallout shelters.

As New York City continues the process of taking down the iconic fallout shelter signs from the New York City Public Schools, some may walk by these signs daily without even knowing they are there. Others may be conscious of their presence given their connection to a time gone by. New York City has adopted the response planning guidance set by [Lawrence Livermore National Laboratory](#) in 2009 for the aftermath of nuclear terrorism. Any concerned or informed citizen can go to the [Plan Now NYC website](#) and find guidance on what to do after a radiological attack. Much like Hawaii, New York City will provide emergency messaging primarily advising the public to cover their noses and mouths to avoid inhalation injury and find shelter inside the closest building.

What This Means Today

For present-day emergency managers, much can be learned from the principles of the Civil Defense era. The Civil Defense Program taught that it is the responsibility of all



levels of government to plan and prepare citizens to respond to an emergency. This program established the precedent that the federal government should and will support a locality after an emergency declaration similar to the Robert T. Stafford Disaster Relief and Assistance Act. It taught that, [“An acceptable program, must be one that is understood by those directly involved in it,”](#) and that hazards must be mitigated to the extent possible to moderate the potential for a massive recovery effort.

In its final days, the Civil Defense Program demonstrated that developing planning efforts and training for specific hazards is highly effective and should be applied to all hazards, paving the way for current planning practices. It is vital that emergency managers continue to plan for all hazards. However, with old threats returning anew, it is important to prepare for a perceived and or imminent threat and focus training to reduce it. The Civil Defense Program highlighted that “the best defense is often a good offense,” as seen in the current Hawaiian education campaign.

Although the most recent false alarm created genuine concerns and issues, the importance of these tests cannot be overstated. Despite the false alarm in Hawaii, the need for and value in regulated and recognized monthly testing should not be ignored. These tests familiarize the citizens of Hawaii with the sound of air raid sirens, making the sound recognizable and providing citizens opportunities to practice recommended actions. The tests familiarize the Hawaii Emergency Management Agency with the notification procedures and highlight areas for improvement. Most importantly, practicing these scenarios will reduce panic, to some degree, at the time of an actual event.

The response to a nuclear event has not changed much over the past 70 years. However, when seeking shelter, one cannot go back to the fallout shelters of yesterday. Instead, they must seek shelter, as quickly as possible, in the closest possible building, or even in the confines of their own homes.

Keith Grossman, MPA, is the director of emergency management for the New York City Department of Education (DOE). In this role, he is responsible for the system-wide emergency planning for the largest school system in the United States consisting of over 1,800 schools in over 1,300 locations. His team is responsible for shaping the role of the DOE in the city-wide response framework, serving as the 24/7 point of contact for the NYC’s emergency services, serving as the logistics chief for the Emergency Sheltering System, and conformity of emergency programs with the American’s with Disabilities Act. Prior to working at the DOE, Keith served as the Director of Emergency Management Safety at Brookdale Hospital in Brooklyn, the Planning Section Chief at Brookhaven National Laboratory and the Emergency Management Coordinator at Nassau University Medical Center. Keith holds a Bachelor of Arts from Binghamton University, a Graduate Certification in Emergency Management from Adelphi University and a Master of Public Administration from Alfred University.

U Visas – A Hidden Homeland Security Vulnerability

By Robert C. Hutchinson

Immigration continues to be a relevant yet sensitive topic of discussion. Some of the most concerning immigration issues may be the ones that are more complex and not well understood by lawmakers, law enforcement, or the public. This complexity increases opportunities for abuse of an important immigration process, which then creates a significant vulnerability that is not fully appreciated until it is too late.

The U nonimmigrant status (U visa) application process presents a hidden threat that may not be properly analyzed and addressed until well after a critical event. At that point, questions will arise about the warning signs that were not addressed long before the terrorist attack or high-profile criminal act.

U Visa Application Process

According to U.S. Citizenship and Immigration Services (CIS), the [U visa](#) is reserved for victims of certain crimes who have suffered mental or physical abuse and are helpful to law enforcement or government officials in the investigation or prosecution of criminal activity. As a result of the passage of the [Victims of Trafficking and Violence Protection Act](#) in October 2000, the U visa was created to strengthen the ability of law enforcement agencies to investigate and prosecute cases of domestic violence, sexual assault, trafficking of aliens, and other crimes, while protecting victims of crimes. Some of these victims have suffered substantial mental or physical abuse due to the crime and are willing to help law enforcement authorities in the investigation or prosecution of the criminal activity. According to CIS, the legislation also helps law enforcement agencies to better serve victims of crimes.

The [CIS website](#) states that an alien may be eligible for a U visa if:

- He or she is the victim of qualifying criminal activity;
- He or she has suffered substantial physical or mental abuse as a result of being a victim of criminal activity;
- He or she has information about the criminal activity (If under the age of 16 or unable to provide information due to a disability, a parent, guardian, or next friend may possess the information about the crime on his/her behalf);
- He or she was helpful, is helpful, or is likely to be helpful to law enforcement in the investigation or prosecution of the crime (If under the age of 16 or unable to provide information due to a disability, a parent, guardian, or next friend may assist law enforcement on his/her behalf);
- The crime occurred in the United States or violated U.S. laws; or
- He or she is admissible to the United States (if not admissible, he/she may apply for a waiver).

The U visa is valid for four years, with extension eligibility if another immigration adjustment or status is not granted during that time. The approved applicant is eligible to apply for a [lawful permanent resident](#) card (green card) after three years – a pathway to citizenship.

A limit of 10,000 U visas per year is set for principal petitioners, but there is no cap for their family members deriving status from the applicant. When the annual cap is reached, CIS creates a waiting list pending a final decision. Applicants and family members on the waiting list are granted deferred action or parole and are eligible for work authorization, which permits them to remain in the United States until their petition can be reviewed by CIS.

U Visa Statistics & Congressional Interest

According to [Department of Homeland Security \(DHS\) statistics](#), 60,710 U visa applications were received and 17,937 were approved in fiscal year 2016, with a backlog of 150,561 to be adjudicated by CIS. [CIS statistics](#) show that 35,044 petitions were received in fiscal year 2016. Out of those U visa petitions, 10,046 were approved, 1,843 were denied, and 23,155 were pending review. The total number of U visa petitions pending review from fiscal years 2009 to 2016 is 86,980.

From those 35,044 victim requests in fiscal year 2016, an additional 25,666 family members also applied for the status along with the victim of criminal activity applicants – 7,891 family members were approved and 1,318 were denied by CIS. The total number of family member U visa petitions pending review from fiscal years 2009 to 2016 is 63,624.

In December 2016, Senate and House Judiciary Committee Chairmen identified [significant fraud](#) within the U visa program through falsified applications and disregard of congressional limits for the program. According to congressional findings, recent cases have highlighted how the program is being exploited through falsified police reports and bribes to secure U visas, allowing foreign nationals to avoid deportation. Whistleblowers report that illicit activity to secure U visas is common.

The oversight of this little known program has reportedly been insufficient, permitting its extensive improper utilization and extended delay of deportation for many well beyond the legal limits and eligibility for the program. As a result, the program could be leveraged not only by criminal aliens, but those who wish to do even greater harm.

Document Verification & Fraud

Beyond the good intentions of the U visa program, investigative reporting and research have identified broad and widespread abuses of the U visa process, with fraud and abuse perpetuated by incorrect or inconsistent information provided to or possessed by law enforcement and prosecutors. With no statute of limitations for the reported crime or victimization, it is even more difficult for the certifying officials to determine helpfulness or the actual role of the aliens for alleged crimes that are decades old.

Even though DHS has issued [U visa reference resources](#), the application process may not be well understood by the thousands of law enforcement agencies, prosecuting attorneys, and nongovernmental organizations requested to assist with the applications. Checks and balances are needed between CIS and the certifying officials and agencies, including confirmation of the number of petitions submitted and received each year from the agency. Without them, CIS could process applications with fraudulent information and counterfeit signatures without the certifying official knowing of the submitted false petitions.

In addition to the challenges encountered by the law enforcement agencies and prosecuting attorneys, CIS may not be able to verify all the authorizing officials and their signatures on thousands of petitions with so many agencies involved in the process across the country. It is often difficult when dealing with one large organization over time with policy, authority, position, and official changes to ensure that the submissions are true and factual. Due to this situation, there is ample room for fraud with the limited CIS verification resources.

Beyond the challenges of those wishing to support this well-intentioned program, many document and benefit fraud investigations have verified attorneys and public officials abusing the U visa process. For example, an attorney and a police officer were [reportedly indicted in 2016](#) along with others for submitting fraudulent documents to CIS to obtain U visas for other co-defendants during a marriage fraud scheme. Similar violations may be more prevalent than reported.

Unexpected Consequences

The U visa process has reportedly been utilized to release aliens from immigration detention prior to scheduled deportation due to questionable claims, documents, and/or incidents. Information indicates that certain groups, notaries, and attorneys have utilized this process with successful results and profits. The lack of formal and consistent nationwide training and guidance provided to state and local law enforcement, prosecutors, courts, and nongovernmental organizations create confusion and opportunities for error and abuse.

Aliens smuggled into the United States could also utilize the process. For example, an alien smuggled into the United States is held at a load house pending release to their family or friends. The alien does not wish to pay for the smuggling venture or an unexpected fee increase, so he contacts a family member for assistance. The family member contacts law enforcement to report that his family member is being held against his will by the smugglers. When located and rescued by law enforcement, the alien could be offered a U visa as a victim of hostage taking or other crimes, since smuggling is not a qualifying U visa crime. This scenario provides a free or reduced smuggling fee and a solid immigration status to remain in the United States.

Another possible scenario involves two illegal aliens involved in an unsuccessful illegal narcotic transaction. For example, a drug buyer and/or seller injured after a robbery or assault of each other during the illegal transaction could be eligible for a U visa as victims of assault and other crimes or as witnesses against each other; they could even apply from jail. This scenario has reportedly occurred and benefited illegal aliens involved in criminal violations. Such victims could be eligible for the benefit if not fully vetted by the different agencies and parties involved in the review and submission process.



Domestic violence is one of the primary crimes utilized in many U visa claims. However, John Sampson, a retired U.S. Immigration and Customs Enforcement (ICE), provided written testimony to the Senate Committee on the Judiciary describing immigration fraud as having reached an “epidemic” level. Such fraud includes using U visas to expedite lawful permanent resident (green card) status during alleged marriage fraud schemes and alleged domestic violence situations.

Retired ICE Special Agent in Charge Claude Arnold identified the enormous value of the [Violence Against Women Act of 1993](#) and U visa process in getting the abused much needed protection, but sees the challenges of the program. In 2011, Arnold stressed that, “[Visa fraud is a serious crime](#). Not only does it undermine the integrity of our legal immigration process and penalize those who abide by the law, it also poses a significant security vulnerability.”

Need for Expanded Oversight

The examples listed above are just a few specific abuses of the U visa program. More examples and concerns such as CIS reportedly not sharing fraudulent petitions and information with ICE due to the alleged victim status of the applicant or when a petition is formally rejected by CIS. With significant confusion and misunderstanding of the process, it is easy to exploit a valuable program that is free to applicants.

Beyond the confusion experienced by state and local agencies and nongovernmental organizations when entering and executing the process, U.S. Customs and Border Protection, ICE, and CIS do not always have common visibility of the process and applicants. DHS internal rules and regulations do not always promote and enhance cooperation and collaboration within the department. There is a serious need for expanded awareness, training, coordination, and collaboration between DHS agencies in conjunction with state and local agencies and nongovernmental organizations.

It is critical for Congress and DHS to ensure that this essential and valuable program is properly monitored and managed and not a conduit for nefarious uses – such as retrieving vital members from detention or deportation and returning them to their assignments, whether criminal or terrorism in nature.

As so aptly stated by President Theodore Roosevelt in his [1913 autobiography](#), “Americans learn only from catastrophe and not from experience.” It would be wise to understand and address this hidden vulnerability before it becomes the topic of numerous congressional hearings and the 24-hour news cycle, which could threaten or overly restrict the U visa program. Actions can be taken before a catastrophe through enhanced attention, comprehensive training, and robust oversight. The time is now to fix the problems.

Robert C. Hutchinson is a former deputy special agent in charge and acting special agent in charge with the U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement’s Homeland Security Investigations in Miami, Florida. He retired in 2016 after more than 28 years as a special agent with DHS and the legacy U.S. Customs Service. He was previously the deputy director and acting director for the agency’s national emergency preparedness division and assistant director for its national firearms and tactical training division. His writings, interviews and presentations often address the important need for cooperation, coordination and collaboration between the fields of public health, emergency management and law enforcement. He received his graduate degrees at the University of Delaware in public administration and Naval Postgraduate School in homeland security studies.

Preparedness Can Be Easy

By Raynika Battle

For more than a decade, Federal Emergency Management Agency (FEMA) statistics have shown that, although there has been some improvement, not enough people are prepared for emergencies and disasters. However, publicly available resources are educating community members and helping them prepare – one month at a time – for potential disasters that are likely to affect them.



FEMA's 2017 [National Preparedness](#) report states that the nation as a whole faces a persistent challenge of inspiring individuals to prepare for emergencies. Even with the use of technology such as social media and mobile applications, getting people to prepare is still tough. In 2015, [FEMA reported](#) that only 39% of respondents had developed emergency plans and discussed them with their households. This is in contrast to the fact that about [80% of Americans](#) live in counties that have been damaged by weather-related disasters in the past.

Building a disaster-resilient community is essential in the process of recovering from a disaster. However, significant amounts of people are still not aware of the potential hazards around them. For example, only 30% of people living in areas historically known for [wildfires](#) are likely to have read or heard about information on how to prepare for a wildfire emergency. Assessing risks has to be personalized. Individuals, families, and businesses have to understand not only how to respond to a disaster but how it will affect them. With the increased frequency of all types of disasters, there has to be a greater sense of urgency in helping communities prepare.

Moving People Forward

Perceptions that it is too hard or too expensive – or they do not know where to start when it comes to preparing for emergencies and disasters – need to change. [Do1Thing](#) combats these barriers by offering a program that is easy, accessible (translated into seven different languages, offered in audio, video, large print, braille, and low-literacy formats), and requires little to no money to build a personalized emergency plan. The goal is to approach the entire community as a whole so everyone can be ready for an emergency.

Emergency preparedness requires an awareness-to-action approach. It is not enough just knowing what to do, but rather taking action to prepare oneself in case of a disaster. Although responders are on call and willing to help, people are responsible first for their own safety. The more individuals prepare, the less demand there is on first responders.

One goal of Do1Thing is to make better disaster decision makers, as no two disasters are the same. When people begin to think about how they would respond to a disaster based on whether or not they are at home, work, or school, it allows them to make better informed

decisions. From those decisions, people can overcome the normalcy bias – the state of mind that takes too lightly the effects of a disaster – and can respond appropriately. This goes beyond telling people what materials are needed in an emergency kit, but getting them to think about how they should respond to different types of emergencies. It encourages consideration of existing special and unique needs – for example, pets, children, special health needs – and what to do about them during emergencies.

How It Works

Started by a local group of emergency managers in 2005, the original intent of Do1Thing was to increase the effectiveness of preparedness for those in the area. It was intended to be a one-time project: once the information was distributed, mission accomplished. However, the program grew into a nationally recognized program for its inclusive preparedness efforts to better prepare individuals, businesses, and children.

Individuals – Do1Thing offers 12 monthly topics that teach people how to do one thing each month to build their emergency plans. Each month, from the three tasks presented, participants choose one to complete. By the end of the year, individuals, families, and businesses will have a plan specific to their needs. For example, February’s topic is “water,” with the following tasks to choose from:

- Purchase and store a 72-hour (or up to two weeks) supply of bottled water.
- Bottle a 72-hour supply of water at home.
- Learn how to provide a safe supply of water for your household in a disaster.

After selecting one task, a few additional details are given so that individuals are clear on what it takes to create a necessary supply of water. For example, additional details explain the need to have at least one gallon of water per person, per day on hand (see Figure 1). Breaking down a complete emergency plan into small easy steps removes barriers and promotes action.



Fig. 1. Example of additional details provided for the water task (Source: Do1Thing, 2018).

Businesses – Businesses also have a place in the preparedness program. The 12 monthly topics are designed to help small-to medium-sized businesses continue operations during and after a disaster. The sooner businesses reopen after a disaster, the sooner people can return to work, the economy can recover, and the community can rebuild. For example, the goal of June’s topic “key personnel” is to identify key personnel and make

sure that at least one other person could step in and do their jobs in the event they are unable to work:

- Identify personnel who perform essential functions in your business.
- Create a succession plan.
- Cross-train employees in critical operation skills in case a key employee is unable to come to work.

Many small businesses have key personnel who are the only people able to perform specific tasks, such as accessing certain systems or even unlocking doors. Making sure that more than one person knows what to do is a key part of surviving after a disaster.

Children – It is never too early to begin talking to children about what to do in case of an emergency. Do1Thing partnered with the Michigan State police to create a kids preparedness coloring book (see Figure 2). The book covers the same 12 monthly topics as those for individuals. The intent is for parents to sit down with their children and discuss what to do during and after a disaster in a kid-friendly format.



Fig. 2. Advertisement for children's preparedness coloring book (Source: Do1Thing, 2018).

Small Steps for Big Planning

Taking small steps toward preparedness helps remove the anxiety, stress, and worry around becoming prepared for emergencies and disasters. Preparedness can be easy, but there has to be an acknowledgment that people have a choice when it comes to their preparedness efforts. This provides a sense of responsibility, empowerment, and engagement in the disaster decision-making process. Disaster outcomes can be improved when people are educated on how to remove common barriers to preparedness. Planning for an emergency does not have to be an astronomical task, but rather a task that is manageable for anyone to do.

Raynika Battle is the executive director of Do1Thing. With a passion for nonprofit management, her experience provides several years of nonprofit and community services work in the Lansing, Michigan, area. She holds a Bachelor of Arts degree from Michigan State University in Political Theory & Constitutional Democracy. She also holds a Master of Science degree from Capella University in Human Services and Non Profit Management. In addition, she has a post-graduate certificate in Strategic Management from Davenport University, and two certificates from Liberty University in Biblical Studies and Biblical Leadership. She is currently pursuing her Professional Emergency Manager (PEM) certification with the Michigan State Police Emergency Management and Homeland Security Division. She is a Community Emergency Response Team (CERT) member and certified by the Red Cross in Disaster Mental Health.



WE STEPPED UP SO YOU CAN STEP BACK.

The new **FLIR identiFINDER® R440** lets you scan for radiological threats from farther away to keep you and your community safe.

The new R440 is a lightweight, sourceless RIID that can be operated with one hand and is IP67-rated to survive tough missions. Not only does the 2x2 NaI detector deliver sensitive and fast detection, but it also provides accurate identification during secondary screening. The new 360° EasyFinder™ Mode expedites decision-making to keep you safe.

[Learn more at flir.com/R440](http://flir.com/R440)



FLIR identiFINDER R440
Highly Sensitive, Sourceless Handheld RIID

