



DomPrep Journal

[Subscribe](#)

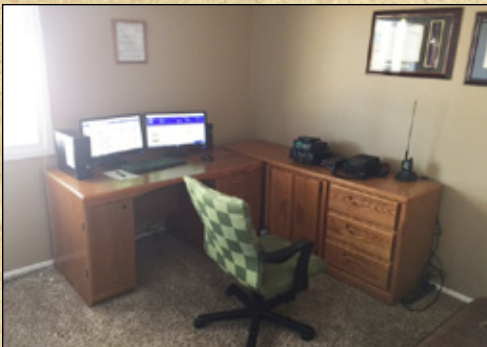
Volume 14, Issue 2, February 2018



2017 Inauguration & Women's March – Planning & Outcomes
By Natalie Jones-Best



New Emergency Rule: Challenge for Some, Good for All
By David Reddick & Justin Snair



Tribal Ham Radio Operators Cut Through the Storm
By National Tribal Amateur Radio Association



Podcast: Hurricane Recovery – The Price of Paradise
Moderated by Andrew Roszak



Passenger Egress – A Priority for Metro Rail Lines
By Thomas Renner



Evolving Needs: Interoperable Communications
By The Metropolitan Washington Council of Governments' Interoperable Communications Regional Programmatic Working Group



Explosives & Handheld Trace Detection
By Ryan Holland & Mark Fisher



Emerging Homeland Security Issues – A 2017 Panel Review
By Joseph J. Leonard Jr.



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](https://flir.com/R440)



FLIR identiFINDER R440
Highly Sensitive, Sourceless Handheld RIID



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:

BioFire Defense

Business Resilience Conference

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

Setting Examples for Disaster Preparedness
By Catherine L. Feinman5

2017 Inauguration & Women’s March – Planning & Outcomes
By Natalie Jones-Best6

New Emergency Rule: Challenge for Some, Good for All
By David Reddick & Justin Snair10

Tribal Ham Radio Operators Cut Through the Storm
By National Tribal Amateur Radio Association14

Podcast: Hurricane Recovery – The Price of Paradise
Moderated by Andrew Roszak15

Passenger Egress – A Priority for Metro Rail Lines
By Thomas Renner16

Evolving Needs: Interoperable Communications
By The Metropolitan Washington Council of Governments’ Interoperable Communications Regional Programmatic Working Group19

Explosives & Handheld Trace Detection
By Ryan Holland & Mark Fisher21

Emerging Homeland Security Issues – A 2017 Panel Review
By Joseph J. Leonard Jr.25

Pictured on the Cover: (top row) Jones-Best, Source: Ted Eytan, 2018; Reddick & Snair, Source: Lauren Hobart/FEMA News, 2002; (second row) National Tribal Amateur Radio Association, Source: Nathan Nixon, 2018; Roszak, Source: DomPrep, 2018; (third row) Renner, Source: Dan Arnold, 2018; The Metropolitan Washington Council of Governments’ Interoperable Communications Regional Programmatic Working Group, Source: ©iStock.com/MaboHH; (bottom row) Holland, Source: FLIR, 2018; Leonard, Source: ©iStock.com/RoschetzkyistockPhoto

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



Setting Examples for Disaster Preparedness

By Catherine L. Feinman



From coast to coast, communities across the United States are implementing solutions to address gaps that could hinder response efforts should a disaster occur. From special events to widespread natural disasters, this edition of the *DomPrep Journal* shares experiences and lessons learned from those who have firsthand accounts of these events and incidents and want to ensure that any existing gaps are closed before similar situations arise within their communities or elsewhere.

On the East Coast, Washington, D.C., offers innumerable opportunities to practice local and regional preparedness, with multiple agencies working together and communicating across disciplines on a daily basis. With thousands of special events occurring in the nation's capital each year, there are many opportunities to practice preparedness. For example, in 2017, [transportation statistics from two events](#) on consecutive days – the Presidential Inauguration and the Women's March – highlight the differences in transportation planning efforts and subsequent outcomes. The National Capital Region, which includes the District of Columbia, continually reviews and practices its plans – including [interoperable communications](#) – during such multijurisdictional events.

On the West Coast, California offers similar preparedness opportunities. In the megacity of Los Angeles, ensuring safe [passenger egress](#) from underground rail lines is a priority. For tribal communities in California and around the country, communications are a priority, with [amateur radio operators](#) able to play key roles during disasters.

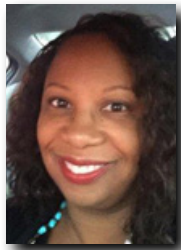
Disasters can occur anywhere and often have far-reaching effects that do not stay confined within jurisdictional borders. As such, regional or national plans may be needed, but can introduce additional challenges for some communities – for example, a [new comprehensive emergency preparedness rule](#) implemented by the Centers for Medicare and Medicaid Services. The 2017 hurricane season exposed other changes that may be needed in the future – for example, improving the ability to move resources into and out of areas like the [Florida Keys](#) when affected by a hurricane or other disaster.

Protecting the homeland from natural or human-caused threats is not the sole responsibility of the federal government, but rather a joint effort for all levels of the public and private sectors. This could include having mutual aid agreements or regional hazardous materials teams equipped with [trace detection equipment](#) to prevent potential terrorist attacks and to respond as needed. Regardless of the type of threat, all emergency preparedness and [homeland security stakeholders must remain vigilant](#), be involved in the planning process, and be ready to respond.

2017 Inauguration & Women’s March – Planning & Outcomes

By Natalie Jones-Best

Washington, D.C., hosts thousands of special events each year, ranging in size and complexity. For such events, the District of Columbia’s Department of Transportation (DDOT) serves as the lead agency for transportation management and support. Although many of these events are planned activities for which the district and its local, regional, and federal stakeholder partners have advance notice for planning purposes, the nation’s capital is also home to many unplanned First Amendment events, which provide less notice and are less defined with respect to the planning and support required. The 2017 presidential inauguration and subsequent Women’s March highlight the differences in planning efforts and outcomes for these two types of events.



One unplanned First Amendment event, the 2017 Women’s March on Washington, illustrates how communities and planning entities can be at a disadvantage by the size and complexity of events where traditional leading indicators provide limited insights for pre-operational planning. The Women’s March took place one day after the 2017 presidential inauguration. Both events revealed the drastic difference between a planned event and an unplanned event that evolves through a grassroots approach supported by social media and word of mouth. With the latter event, one must ask whether this is the new norm for special events.

Guiding Principles for Inaugural Events

DDOT’s inaugural planning efforts have morphed over the years into a somewhat routine planning effort, where roles and responsibilities fluctuate between traditional and nontraditional transportation management tasks. This successful process relies on best practices employed in past events, and lessons learned through after-action reports that allow DDOT to leverage existing frameworks and work with a few key guiding principles in mind for its operations plan.

DDOT recognizes that many event attendees are not familiar with the district landscape. In addition, many of the support personnel from other states are unfamiliar with the district. To assist, DDOT works with its partners to identify appropriate walking routes through wayfinding signage, maps, and public communication channels. The walking routes are part of an overall effort to provide the public with modal alternatives that discourage the use of personal automobiles when high attendance numbers and many parts of the transportation network in the district and surrounding areas are impacted by increased traffic congestion and route closures. For the 2017 inaugural event, the district developed a pre-event “Don’t Even Think about Driving” advertising campaign.

For this campaign, the district provides a turnkey charter bus system that provides registration, vehicle tracking, and parking management of charter buses. Additionally, the district encourages the use of public transportation, including Metrorail and Metrobus, Streetcar, Circulator, Amtrak, and commuter rail, all of which run enhanced schedules for

inaugurations. For the most recent inauguration, DDOT and the District Department of For-Hire Vehicles designated temporary taxi stands and coordinated with transportation network companies such as Lyft, Uber, and Via to implement geofencing technology for identified passenger drop-off and pick-up areas close to events, but away from the most congested areas. DDOT also provided significant support for bicycles during this most recent event by establishing valet bike parking for personal bikes and bike corrals for Capital Bikeshare users.

Variables to Consider in Planning

In contrast to the static planning tasks, the district has formulated assumptions for variables using past data and long-term forecasts. For the presidential inauguration, these variables range from attendance forecasting early in the planning process – resulting in early quantifying of resources and staffing – to involvement of special interest groups, January weather, vehicle access restrictions as determined by federal and local law enforcement entities, and potential security threat levels.

Critical to the planning process is quantifying inaugural attendance levels, which is the most critical variable. Attendance levels can vary significantly. They have a large impact on resource planning and logistics and are affected by many factors, such as whether the event is for a first or second presidential term. Traditionally, attendance is significantly higher for first-term inaugurations. There are significant transportation leading indicators that assist in forecasting attendance levels, including:

- The number of charter bus parking permits issued;
- Hotel bookings within the Washington, D.C., region; and
- Intercity travel bookings (air, rail, bus).

Although methods exist to track projected attendance levels for planned events, and have proven reliable, more challenging is the prediction of attendance for large unplanned events like the Women’s March. The Women’s March evolved rather quickly, and saw significantly more spontaneous attendance.

For instance, the district uses RFK Stadium as its primary bus staging location for inaugural events, with a capacity of 1,300 spaces. Although there are other smaller, less formal staging areas in other parts of the district, there were 200 charter bus permits issued for RFK Stadium for the 2017 inauguration, whereas analysis confirmed 1,200 permits were obtained for the Women’s March (see Figure 1).

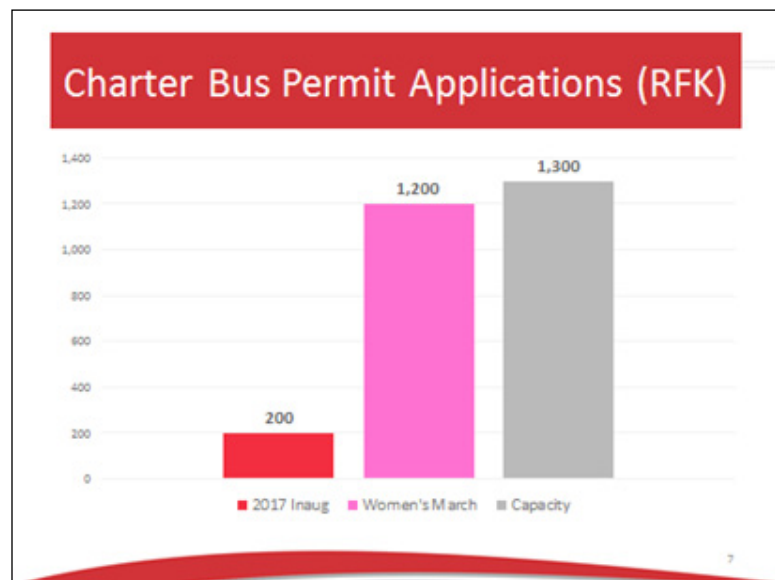


Fig. 1. Number of Charter Bus Parking Permit Applications for RFK Stadium (Source: DDOT, 2017).

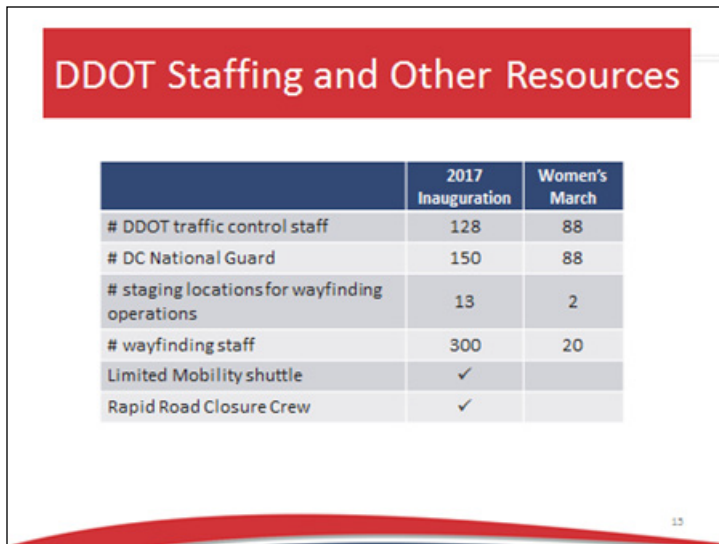


Fig. 2. DDOT Staffing and Other Resources (Source: DDOT, 2017).

The data in Figure 1, conjoined with DDOT’s staffing and resource data, are indicative of how both events were planned for regarding resource allocations. Due to attendance generally rising at inaugural events over the years, DDOT and other agencies had nearly 600 personnel deployed for roadway and pedestrian management, and as ambassadors in support of the inaugural events (see Figure 2). Forced to rely on known information about attendance for the Women’s March, and a scaled down area of coverage responsibility, about a third of the manpower deployed for the

inauguration was requested in support of the Women’s March. It should be noted that, with a nonplanned event evolving from social media and a grassroots effort, traditional indicators are helpful, but do not provide a full operational picture. Consequently, staff levels were reduced based on the known and verifiable information available before the event.

Estimated Crowd Size

Although there is no official estimate of crowd size from the National Park Service regarding the 2017 inauguration, crowd scientists at Manchester Metropolitan University in Britain analyzed photographs taken of the National Mall and vicinity. According to Manchester Metropolitan University, the crowd on the mall area the day of the Women’s March was more than three times the size of the crowd in the hour leading up to the 2017 inauguration speech.

DDOT’s response to the larger crowd for the Women’s March relied on real-time situational awareness, traffic cameras, and in-field support. Working with sister agencies such as the Metropolitan Police Department and the National Guard, DDOT was able to leverage and deploy its operations teams to provide vehicular and pedestrian traffic management for DDOT’s designated coverage area (see Figure 3).

Lessons Learned

Communities preparing for large-scale First Amendment events need to be as proactive as possible in determining a transportation management



Fig. 3. Washington, D.C., Metro station during Women’s March (Source: Ted Eytan, 21 January 2017).

strategy that plans for the unknown and unpredictable. In response to the rise in the number of such events, the district has developed scalable event plans to help with resource deployment. Additionally, communities and special event stakeholders need to closely monitor traditional predictors of attendance and forms of modal access attendees use to reach events, as well as new nontraditional predictors. Traditional metrics like hotel bookings and intercity travel bookings are a starting point, but alternative lodging booking sites such as Airbnb must be factored in some way. Communities must also consider new forms of travel like Uber and Lyft, which provide useful data, in addition to the analysis and monitoring of trending subjects on social media sites that include Facebook, Twitter, Instagram, and LinkedIn.

Although 2017 may prove to be an outlier given the confluence of historic events associated with the two-day period, the experience provides tremendous insight for communities that must now prepare for the growing number of spontaneous First Amendment demonstrations.

Natalie Jones-Best currently serves as the emergency preparedness and risk manager for the District of Columbia's Department of Transportation (DDOT). In her position, she is responsible for managing the transportation emergency responses coordinated under the District of Columbia Emergency Response Plan and overseeing all aspects of DDOT's Emergency Program. During her tenure with DDOT, she has also served as a transportation specialist with DDOT's Office of Mass Transit, working on such issues as light rail development and transit planning, as well as overseeing the department's Federal Grant Program. Prior to joining the district government, she served as an administrative manager with Ryder/ATE, formerly a national transit contracting company and subsidiary of the Ryder Corporation. Her 20-year transportation career has also included serving as a consultant conducting triennial reviews for the Federal Transit Administration and working on a robust transit bus study for the New York Metropolitan Transit Authority. She received her undergraduate and graduate degrees from the University of Virginia, in English and Urban Planning, respectively.



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

The poster features a dark background with glowing blue and yellow virus-like structures. In the background, there are faint images of people in hazmat suits. At the bottom left is a circular seal with an eagle and the text 'DOMESTIC PREPAREDNESS'. At the bottom right is the website 'JOINTCBRN.DSIGROUP.ORG' in large, bold, blue letters.

New Emergency Rule: Challenge for Some, Good for All

By David Reddick & Justin Snair

The Centers for Medicare and Medicaid Services (CMS) implemented a comprehensive emergency preparedness rule in 2016 that applies to nearly every healthcare provider in the nation, and outlines steps those providers must take to improve their preparedness and ensure sustainability in the face of a disaster. The rule compels healthcare providers to devote resources – human and fiscal – to emergency planning. This may be seen as burdensome by some but should effectively improve their levels of readiness and improve the quality of healthcare for all. This rule will make providers – from general hospitals to transplant centers and long-term care facilities – safer for patients and visitors.



Although most people outside healthcare have little awareness of the rule or its requirements, there are good reasons everyone should understand, as they and their loved ones will benefit from enforcement of the rule. Describing the effects of Hurricanes Harvey and Maria in a November 2017 [HomeCare Magazine](#) article, Healthcare Ready Executive Director Nicolette Louissaint wrote, “the devastating and significant impact these events had on health care systems reminds us why it is imperative to have emergency preparedness systems in place to ensure the well-being of patients and providers during a disaster.”

Her group, along with others, has spent the past months promoting the emergency rule and encouraging healthcare providers to expand their planning to ensure compliance. Sessions on the rule at a November 2017 National Healthcare Coalition Preparedness Conference in San Diego, California, were popular draws, with more than 60 people attending a half-day workshop co-sponsored by Louissaint’s Healthcare Ready, FEMA’s Center for Domestic Preparedness (CDP), and Bio-Defense Network. A panel discussion later in the conference – featuring representatives of CMS, the California Department of Public Health, and Healthcare Ready – drew a standing-room-only crowd.

Key Elements of the Rule

The FEMA CDP has become a chief source of information on the rule, scheduling dozens of comprehensive and complimentary onsite two-day workshops around the nation for providers and healthcare coalitions. In addition to CDP and CMS, significant support for providers has been made available through the U.S. Department of Health and Human Services (HHS) Assistant Secretary for Preparedness and Response’s Technical Resources, Assistance Center, and Information Exchange ([TRACIE](#)) service. TRACIE has also produced a series of frequently asked questions and conducted webinars designed to [answer questions](#) being raised by providers across the nation.

The rule contains four primary elements, each of which feeds into an organization’s overall emergency preparedness program:

- *Risk Assessment and Planning* – Requires providers to assess specific and general risks they face and create plans to respond to those risks.
- *Policies and Procedures* – Must be written, approved, and reviewed on a regular basis, at least annually.
- *Communications Plan* – Must be created and outline how a healthcare provider will communicate both internally and externally, especially when normal means may be unavailable.
- *Training and Testing* – Requires providers to train their staff and conduct periodic testing and exercises to ensure they can do what they must do in the event of a disaster.

These elements sound familiar to business continuity and emergency preparedness professionals, but are not second nature to many healthcare providers, whose backgrounds are focused on healing and medical treatment, not preparedness. This may be why so many providers find themselves in a quandary when faced with complying with the rule. Many providers already do much of what is being required, but full compliance is still necessary, and failure could eventually jeopardize a provider's Medicare and Medicaid funding.

The importance of this rule became clear after Hurricane Irma in 2017, when a dozen people from a Florida nursing home died from “environmental heat exposure.”

Different Providers, Varying Requirements

CMS has taken significant steps to promote and explain the requirements by conducting numerous webinars and having representatives speak at multiple events. However, many recipients remain unclear about the steps they must take, how they should document those steps, and what full compliance will look like for them.

Part of the lack of clarity is because 17 different provider and supplier types (see Table 1) are covered and, although there must be general compliance, nuances exist among them, for example:

- Outpatient providers are not required to have policies and procedures for the provision of subsistence needs;
- Home health agencies and hospices must inform officials of patients in need of evacuation; and
- Long-term care and psychiatric residential treatment facilities must share information from the emergency plan with residents and family members or their representatives.

These requirements are not universal for the 17 provider types. Adding to the complexities, advance copies of the all-important Interpretive Guidelines and Survey Procedures were released in the middle of 2017 – just five months before all recipients were expected to be in full compliance.

Table 1. Providers/Suppliers: Facilities Impacted by the Emergency Preparedness Rule

1	Hospitals
2	Religious Nonmedical Healthcare Institutions
3	Ambulatory Surgical Centers
4	Hospices
5	Psychiatric Residential Treatment Facilities
6	All-Inclusive Care for the Elderly
7	Transplant Centers
8	Long-Term Care Facilities
9	Intermediate Care Facilities for Individuals with Intellectual Disabilities
10	Home Health Agencies
11	Comprehensive Outpatient Rehabilitation Facilities
12	Critical Access Hospitals
13	Clinics, Rehabilitation Agencies, and Public Health Agencies as Providers of Outpatient Physical Therapy and Speech-Language Pathology Services
14	Community Mental Health Centers
15	Organ Procurement Organizations
16	Rural Health Clinics (RHCs) and Federally Qualified Health Centers
17	End-Stage Renal Disease Facilities

Healthcare coalitions have become key players in promoting the rule. Many have seen increases in membership from providers seeking help in their planning efforts and involvement, especially in the areas of policies and exercises. In addition, the overall interest in the rule has become clear to national leaders such as Jennifer Pitcher, executive director of the MESH Coalition in Indianapolis, a lead organizer of the National Healthcare Coalition.

“MESH Coalition has continually experienced an increase in national contacts with regard to resources and calls for assistance,” Pitcher said in an email, citing what she called an “incredibly encouraging” level of interest apparent last November 2017 at the group’s annual preparedness conference. “We are excited for the energy that the rule has brought within our healthcare community and look forward to the successful response as a direct result to those collaborations.”

A key requirement of the rule deals with temperature controls and emergency and standby power for hospitals, critical access hospitals (smaller facilities, often located in rural areas), and long-term care facilities. The importance of such controls and backups was made clear in South Florida in 2017, when a dozen people from a Hollywood Hills nursing home died after Hurricane Irma – as the result of what police termed “environmental heat exposure.” The facility’s emergency generators operated as expected when utility company power was lost, but they were powerful enough to provide only light and other basic power. Since it did not generate enough power to keep the air conditioning system running, residents suffered in the stifling heat for three days following the storm.

Most facilities must include evacuation procedures as part of their emergency program, but some smaller facilities do not have this requirement. As such, the staff at the nursing home monitored the residents for heat exhaustion and attempted to keep them comfortable. However, three days lapsed – and nine residents died – before the decision was made to move the patients to a hospital trauma center directly across the street. The deaths of three more residents also were attributed to the heat after they were moved to the hospital.



Christus St. Mary's Hospital evacuated their patients to other hospitals, due to the Hurricane Evacuation orders preparing for Hurricane Lili (Source: Lauren Hobart/ FEMA News Photo, 01 October 2002, Port Arthur, LA).

Additional Training & Reviews

In the *HomeCare Magazine* article, Louissant cited the past hurricane season as a powerful teacher, which “highlighted the challenges the health care community faces during natural disasters, and underscored why in today’s integrated health care system, it is essential to know and trust community partners before disaster strikes.” The rule encourages providers to create partnerships through the training and exercise component, which “creates an opportunity for health care coalitions to assist their members in compliance.”

As periodic reviews for compliance are undertaken in 2018, it is likely that gaps in emergency planning and execution will be noted, and corrective actions required. It is also likely that some CMS recipients will decry the requirements that they improve their efforts. Nevertheless, it is clear that preparedness will be enhanced, healthcare will be improved, and lives will be saved.

David Reddick, CBCP, is chief strategy officer and co-founder of Bio-Defense Network, a public health preparedness consultancy based in St. Louis, Missouri, and Mesa, Arizona. He has more than four decades of experience in communications, business continuity, and public health preparedness. He holds a certificate in emergency management and crisis leadership from Saint Louis University, where he is studying for a Master of Public Health degree, with a focus on biosecurity and disaster preparedness.

Justin Snair (pictured above), M.P.A., CBCP, is the founder and principal consultant with SGNL Health Security Solutions and co-founder of Naseku Goods. Formerly, he was a senior program officer with the National Academy of Sciences, Engineering, and Medicine and directed the Forum on Medical and Public Health Preparedness for Disasters and Emergencies and the Standing Committee on Medical and Public Health Research During Large-Scale Emergency Events. In 2012-2015, he served as a senior program analyst for critical infrastructure and environmental security at the National Association of County and City Health Officials. For six years, he was the local preparedness director and environmental health agent with the Acton Public Health Department in Massachusetts. In 2001-2006, he served as a corporal and combat engineer in the U.S. Marine Corps Reserves and is a veteran of the Iraq war. He holds a Master of Public Administration degree from Northeastern University's School of Public Policy and Urban Affairs, a Bachelor of Science degree in Health Science from Worcester State University, and is an executive fellow with Harvard University's National Preparedness Leadership Initiative.

Tribal Ham Radio Operators Cut Through the Storm

By National Tribal Amateur Radio Association

In September 2017, the National Tribal Amateur Radio Association (NTARA) – in conjunction with the Fresno Amateur Radio Emergency Services Group and Tulare County Amateur Radio Club – set up and operated Amateur Radio Special Event Station W7NTV during the National Tribal Emergency Management Council (NTEMC) annual conference. Held at the Tachi Palace Casino Resort in Lemoore, California, this was the second year that NTEMC and NTARA set up and operated the special event station.



President Nathan Nixon of NTARA, along with several volunteers and NTEMC staff persons manned and operated the station from 9:00 a.m. to 5:00 p.m. daily during the conference, which was held 18-22 September 2017. During that event, the special event station made 312 contacts across the United States, to include places like Hawaii, Canada, and as far away as South America. Each year, this event shines light on the importance of amateur radio emergency communications in tribal communities and demonstrates how, when other communications systems fail during times of disaster, amateur radio can still communicate across the country and the world.

During the conference, a representative from the United States Department of Health and Human Services, Centers for Disease Control (CDC) approached the National Tribal Emergency Management Council's Executive Director, Lynda Zambrano, and asked if there might be any attendees from the Miccosukee Tribe in Florida present at the conference. He was trying to make contact with the tribe, but was unsuccessful due to the Hurricane Irma. Zambrano suggested that, since much of the infrastructure had been compromised, using the National Tribal Amateur Radio Station at the conference might be a more viable resource that he could use. The CDC tribal liaison officer contacted the operators at the special event station to verify if the Miccosukee tribal elders received a physician they requested during the height of the hurricane.

With assistance at the special event station, the operators were able to contact other licensed amateur radio operators in Florida who were able to make contact with the Miccosukee Tribal Police Department. The operators were advised that the electric and phone services in the area had been severely damaged. Through the long-distance amateur radio communications, it was determined that the individuals in the Miccosukee Tribe were unaware of any doctors that had been dispatched or arrived on scene.

This information was provided to the representative from the CDC, who thanked the operators for their dedicated persistence in obtaining the information. This instance is a perfect example of how amateur radio communications can assist tribal communities in times of disaster. This was also the second year in a row that the National Tribal Emergency Management Council and the National Tribal Amateur Radio Association successfully completed coast-to-coast communications using amateur radio in Indian country.

The National Tribal Amateur Radio Association (NTARA) is an Amateur Radio Association dedicated to expanding the role and use of amateur radio in tribal communities. NTARA is open to all licensed amateur radio operators and those who are interested in amateur radio. The goal of NTARA is to provide licensing classes and testing sessions, equipment donations, and work to provide S.T.E.M. as it relates to amateur radio.

Hurricane Recovery – The Price of Paradise

On the morning of 10 September 2017, Irma made landfall in the Florida Keys as a Category 4 hurricane. Mandatory evacuation pushed tens of thousands of people onto a two-lane road. Returning to the area following the storm introduced additional challenges, for example: fuel trucks having trouble entering, housing shortages, landlord issues, builder contract concerns, vulnerable populations, and other reasons for delayed entry. With surrounding areas also being affected by the storm, prioritization and allocation of essential services and shared assets, as well as warehousing of donations proved to be difficult. However, out-of-state workers and resources such as the Incident Management Assistance Teams (IMATs) have played critical roles during the ongoing recovery phase.

As returning to a new normal continues, donor fatigue has set in, but long-term recovery groups have formed and the true recovery is beginning. The misconception that everyone in this service industry town is wealthy can hinder recovery for those in need. On 2 February 2018, DomPrep Advisor Andrew Roszak held an exclusive interview with one Key West resident who reflected on lessons learned as he continues to balance life and work. Living in an RV after losing his home to Irma, J. Matthew Massoud, case manager for Monroe County Social Services, faces these challenges head on and helps prepare his community for a time in the near future when Federal Emergency Management Agency (FEMA) assistance will end. In this podcast, he shares his experience, offers tips for others who may someday find themselves in a similar situation, and provides possible approaches for filling the gaps when federal assistance is no longer available.

[Click to listen.](#)



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



J. Matthew Massoud,
*Case Manager, Monroe County
Social Services, Key West, Florida*



Passenger Egress – A Priority for Metro Rail Lines

By Thomas Renner

Underground rail transit systems in the United States can be dangerous places. Not only for their riders and employees, but also for emergency responders, who may be called to help evacuate people from the area safely or to stop a blaze. The confined spaces, tight stairwells, and potential for the emergency evacuation of hundreds – if not thousands – of riders means that a project must be well-designed, thought-out, and constructed of materials that do not burn.



Code-compliant egress is essential for any building, but underground rail lines make it especially challenging to design a proper egress solution. “Most egress codes are based on walking out of an apartment or a building where a door is three feet wide,” Harold Levitt said during a February phone interview from his New Jersey home. Levitt is a former New York Port Authority of New York and New Jersey employee and a former Manager of Capital Programs for PATH (Port Authority Trans-Hudson Corporation). PATH is a subsidiary of the Port Authority of New York and New Jersey. Levitt is also a former chairperson of the committee that created the language for the National Fire Protection Association Standard [NFPA 130](#), “Standard for Fixed Guideway Transit and Passenger Rail Systems” – the standard that addresses railroad egress. “You could have 1,000 people on a train or in a tunnel. If you don’t have properly planned egress, you’ll have a choke point that could result in an unwanted condition,” he continued.

Providing emergency egress for rail riders and even building crews is one of the top concerns for design and construction teams creating a new rail line in Los Angeles, California. The line includes three underground stations and three at-grade stations will also include emergency doors to allow access to underground control stations. Two stations are above grade.

Plans for the 8.5-mile, \$2.058 billion rail line started shortly after the Los Angeles riots in 1992. The extension is designed to better serve transit-dependent residents in the corridor and provide economic stimulus in the region.

NFPA Sets Rules for Code Compliance

Compliance for underground egress falls under two key codes from the National Fire Protection Association. [NFPA 101](#), Life Safety Code, characterizes platforms and stations as assembly occupancies, with provisions requiring egress systems that facilitate rapid and efficient evacuation, according to an [article in the NFPA Journal](#). This code works with NFPA 130, which specifies fire protection and life safety requirements for underground, surface, and elevated fixed guideway transit and passenger rail systems. The code includes guidelines on fire protection requirements and emergency ventilation systems.

Egress systems also support workers who are constructing the line. Construction is the most dangerous job in the United States according to statistics compiled by the Occupational Safety and Health Administration. The [federal agency reported](#), “5,190 workers were killed on the job in 2016, ... an average of more than 99 a week or more than 14 deaths every day.”

“There have been older stations that were not always compliant with the current code,” Levitt said. “That’s changed over time. Any modification to a station when transit properties agree to do so are upgraded to meet the current code. A number of stations have engineered solutions, such as safe fire zones as in safe areas of refuge to evacuate people from stations more orderly by keeping them behind fire doors/walls. Many stations have thus become substantially safer.”

Doors Designed for Safe Egress

The Los Angeles County Metro Rail System and Walsh/Shea Corridor Constructors, which is building the line, used specialty access doors to comply with the fire code egress laws. The project was specified with six emergency exit hatches and four large doors to access the underground control systems (see slideshow). The hatches and doors are installed all along the lengthy project, which is expected to be complete in October 2019.

The doors are equipped with custom features that make them ideal for use in this application. Each of these heavy doors is supplied with an engineered lift assistance system and a two-point panic locking mechanism that allow the doors to open with less than 30-pounds of force, a critical requirement for safe egress in an emergency.

Emergency egress for rail riders is one of the top concerns for design and construction teams creating a new rail line in Los Angeles, California.

Additional features also need to be added at the ground level where the doors will be installed in sidewalks to ensure reliability and added safety. To prevent structural damage, the doors are reinforced for vehicular loading to withstand the weight of an occasional car or truck that may drive onto the sidewalk. They also feature a slip-resistant coating on the walking surface to ensure safety in these high-pedestrian traffic areas.

Two emergency doors are at underground stations at Expo/Crenshaw, Martin Luther King, and Leimert Park. The stations at Hyde Park, Fairview Heights, Downtown Inglewood, and Westchester/Veterans are at-grade and the Aviation/Century stop is elevated, so emergency evacuation doors are not required.

Increased Need for Swift Egress

Providing code-compliant egress for passengers seems to have become more critical in the past decade. Terrorist attacks and a crumbling infrastructure have made underground transportation particularly hazardous.

The deadliest terrorist assault in rail line history occurred in London on 7 July 2005, when a series of coordinated terrorist attacks killed 52 people and injured more than 700. The tragedy was the first Islamic suicide attack on Britain. Since the London tragedy, there have been more than 15 attacks worldwide, including a blast in 2016 in Belgium that killed 20 people. Potential attacks on U.S. soil in New York (2009) and Washington (2010) were foiled.

Access Doors for Underground Egress

Los Angeles, California

[Click to view album](#)



“NFPA 130 was never meant to deal with terrorism because, when it was established in the 1970s, there was nothing around to consider,” Levitt said. “It’s always an issue because there is no way of knowing what the limits are. Is it an explosive? Biological? Nuclear? It’s very difficult because there is such a wide range of potential threats.”

Inadequate maintenance and costly repairs have also taken their toll on underground transportation. In 2015, riders of the Washington, D.C., Metrorail system subway stopped because of smoke in a tunnel. When smoke seeped into the cars, one woman died and 91 people were injured. The cause of the smoke, according to the National Transit Safety Board (NTSB), was a fire triggered by electrical arcing from a high-voltage rail. The NTSB said the short circuit had gone undetected and unrepaired.

In 2017 in New York, the subway system stopped twice in one day due to track fires. Many of the issues are related to trash on the tracks. New York’s Metropolitan Transportation Authority removes nearly 40 tons of garbage daily from the intricate system, which covers 245 miles across 36 lines and opened in 1904. In 2014, the [MTA reported](#) a staggering 525 track fires throughout its subway system. More than half of the fires (329) involved debris, grease, and garbage.

Updating Infrastructure in Los Angeles

The Los Angeles project is part of a major infrastructure update in advance of the 2028 Summer Olympics. The new projects are designed to increase the use of public transportation and ease congestion on the city’s roadways. The “City of Angels” is also building a nine-mile extension to a Westside subway line and an automated people mover that will serve people on the Crenshaw Line and help them connect to the broader Metro rail network.

While much needed and anticipated, rider and worker safety are of critical importance to the project. Dave Pebley of Specialty Building Components, The BILCO Company sales representative in Pico Rivera, California, feels the Metro Rail Line and Walsh/Shea did their due diligence in taking the proper precautions. “These doors work easily and be are very reliable,” he said. “The owner of the project took the safety of the workers and the riders into consideration very early on. They understood that, in a project like this, safety is paramount.”

Thomas Renner is an award-winning, Connecticut-based journalist who writes extensively on construction and other building trades.

Evolving Needs: Interoperable Communications

By The Metropolitan Washington Council of Governments' Interoperable Communications Regional Programmatic Working Group

During complex and large-scale incidents, first responders in the multi-jurisdictional National Capital Region (NCR) must be able to deploy and integrate with other public safety agencies in a timely and efficient manner. The NCR, for the purposes of this document, is defined as the District of Columbia and surrounding Virginia and Maryland metropolitan areas. Successful integration is contingent on first responders' ability to communicate seamlessly outside the normal coverage area of their home radio systems.



Inter Radio Frequency Subsystem Interface (ISSI) technology allows multiple communications systems to connect and form a single, larger, area-wide network. This “system of systems” technology greatly amplifies capabilities of traditional two-way radios, known as Project 25 (P25) Land Mobile Radio Systems (LMR). When paired with appropriate systems planning and management, standard operating procedures, and recurring training, the ISSI can be an invaluable tool for the NCR to increase the efficiency and reliability of interoperable communications during emergency response.

Benefits & Limitations of P25 & ISSI Technologies

Since 1989, federal, state, territorial, and local public safety agencies have used P25 LMR digital two-way radios, which enable information sharing and communication between multiple users on a single system. P25-compliant radios on one system can also operate on another neighboring P25 system via the Common Air Interface (CAI). However, moving to a neighboring system disconnects users from their home systems and communications with their dispatch centers and agency radios (Figure 1). First responders cite this communications barrier as a primary concern when utilizing P25 radio systems, especially when many first responders using multiple different systems are assigned to a single event.

ISSI technology can help overcome some of the limitations of traditional P25 radios when used as a secondary system. ISSI technology forms a bridge between systems so that users can roam between their home systems and neighboring systems without any disruption in service, similar to a Verizon cellphone customer roaming on the AT&T network when out of range of a Verizon

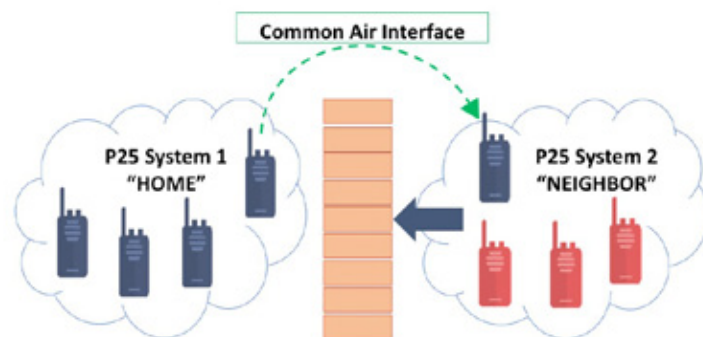


Fig. 1. P25 Land Mobile Radio (LMR) technology (Source: IC RPWG, 2018).

tower. Dispatchers can still communicate with their users even if they have traveled out of the coverage area of their radio systems. Furthermore, all communications crossing the ISSI bridge are digitally encrypted for high performance and security.

Despite these advantages, ISSI technology can impede communication if used or managed incorrectly. The problem is similar to what happens when too many cellphone users try to make calls after a disaster in an area with limited network access. If a network becomes overwhelmed by the number of callers trying to access it, it effectively denies service to everyone who is trying to use it (including that network's paying subscribers).

Similarly, if too many neighboring radio systems try to use the ISSI bridge to connect to another neighbor's home radio system, this will overwhelm the capacity of the neighbor's home radio system to take calls, resulting in a "system busy" signal. System busy signals of this type could shut down all communications and block the home radio system users from accessing their own networks.

ISSI Implementation & Integration: National Capital Region

When used properly with primary P25 LMR radios, ISSI technology is a valuable tool that can facilitate greater interoperability in the NCR. For this reason, NCR stakeholders are currently working together on developing proper governance structures to build a common foundation for all users to use ISSI in a way that does not risk compromising any existing communications systems.

Currently, the NCR, through the Metropolitan Washington Council of Governments' (MWCOC) Interoperable Communications Regional Programmatic Working Group (IC RPWG), is working with jurisdictions and stakeholders to fully integrate ISSI technology as a secondary system and provide regional capacity. The working group is developing a project plan for configuration of ISSI technology with full functional capability before the Washington Metropolitan Area Transit Authority's (WMATA) Metrorail Public Safety Radio System (PSRS) replacement is completed in 2021.

ISSI technology implementation is expanding across the NCR, most notably in Arlington County, Alexandria, Fairfax County, Prince William County, and Loudoun County. WMATA purchased hardware to allow for Metrorail interconnectivity with jurisdictional partners, and additional connections for use with other potential partners such as D.C., Montgomery County, and Prince George's County. Prince William County and Fairfax County tested the ISSI technology to ensure that it functions properly if a P25 system malfunctions and found the test to be successful.

The Interoperable Communications Regional Programmatic Working Group (IC RPWG) brings together the National Capital Region's interoperability partners to enhance the preparedness, responsiveness, and safety of communities by seamlessly sharing data, communications, information, and resources across jurisdiction and discipline boundaries and practicing collaborative decision-making. The IC RPWG works toward this vision by implementing a strategy to address focus areas and objectives of the region, with the support of the Metropolitan Washington Council of Governments (MWCOC) Department of Homeland Security and Public Safety (DHSPS). The MWCOC DHSPS fosters collaboration and provides subject matter experts and decision-makers with the tools needed to make sound financial, resource, and programmatic decisions regarding regional homeland security preparedness, response, and recovery. For further information about ISSI integration within the NCR, please contact Mike Newburn, chair of the IC RPWG, at (703) 883-7050 or Michael.Newburn@fairfaxcounty.gov

Explosives & Handheld Trace Detection

By Ryan Holland & Mark Fisher

The threat of homemade explosives (HMEs) is not new. From the Oklahoma City bombing in 1995, to the “shoe bomber,” London underground bombings, “underwear bomber,” and attacks in Paris and Brussels in the 2000s, the threat is ever changing. Not only do post-incident crime scenes present danger to responders until secondary devices have been ruled out, but also makeshift laboratories where the bombs are made. Handheld explosives trace detection (ETD) equipment can help responders quickly determine on-scene threats, like Triacetone Triperoxide (TATP) and react appropriately and expediently.



TATP has been used in bombing and suicide attacks, including the 2016 Brussels and 2017 Manchester Arena bombings. It was also used in the explosion that preceded the 2017 terrorist attacks in Barcelona. Terrorists frequently use this chemical because it is relatively easy to make using household supplies. As such, TATP is often produced in makeshift laboratories found inside apartments, homes, or other residential structures.

Evidence of TATP manufacture may include glassware such as beakers or flasks, mixers, filtration systems, and distillation equipment. TATP is often kept cold to increase its stability, so ice baths or refrigerators may indicate production. Its instability makes it very dangerous to responders investigating makeshift laboratories. Even trace level quantities can be dangerous if detonated.

TATP Chemical Relevance

Given the instability and volatility of TATP, it is important for responders to know what to look for and how to approach explosion sites or suspected makeshift laboratories where the chemical has been found or handled. TATP appears as a white crystalline powder with a bleach-like odor. Shock, static, sparks, heat, and friction can cause detonations.

Large volumes of easily obtained chemicals such as acetone, sulfuric acid, or peroxide-based bleaching formulations can be indicators of TATP production (Figure 1):



Fig. 1. TATP can be made from commonly available household ingredients (Source: FLIR, 2018).

- Acetone is found in nail polish remover or paint thinner.
- Sulfuric acid is present in car batteries and acidic drain cleaners.
- Cosmetic or wood bleaching solutions can be a source of concentrated hydrogen peroxide.

These ingredients are not just dangerous on their own, but gaseous byproducts produced by them can be toxic and explosive.

Using Explosive Trace Detection

In a suspected bomb-making environment, both surfaces and containers may be investigated using particle or vapor sampling procedures. Responders should always be aware of the possibility of booby traps or secondary devices, and the dangers of entering homemade laboratories.

Numerous technologies can be used for detection, including colorimetric kits (using wet chemistry and color change indicators), Raman spectroscopy (confirmatory tool), ion mobility spectrometry (IMS), and chemiluminescence.

The data provided in this article demonstrates TATP detection using a chemiluminescence-based ETD.



Fig. 2. Vapor-based sample collection and analysis (Source: FLIR, 2018).

Detection of trace explosive signatures results from either directly collecting trace quantities of explosive particles, or by sampling vapor that emanates from an explosive source. Particulates can be solid explosive residue or non-explosive particulates contaminated with explosives, with surface contamination occurring in two primary scenarios:

- When explosives are handled or moved, small particulates of explosives can become suspended in the air and settle onto surfaces.
- Surface contamination can also occur through direct contact with explosive-contaminated or contact with another explosive-contaminated surface. Primary transfer occurs when bulk explosive materials (a quantity that can easily be seen) come into direct contact with a surface, such as a person's hand when handling explosives. Secondary transfer occurs when a surface that was contaminated by primary transfer comes into contact with a second surface.

An example of secondary transfer would be a transfer of explosive materials to an identification card, door handle, cellphone, etc.

Vapor – TATP vaporizes very quickly, resulting in a vapor signature that can be readily detected with a handheld ETD. The vapor enters the sensor via direct vapor sampling (Figure 2). The direct vapor method is effective for screening bottled liquids and concealed, high-volatility explosives.

Vapor becomes more dilute as it travels further from the source and mixes with the surrounding air, resulting in lower concentrations of explosives. Vapors can accumulate to higher concentrations in confined spaces, such as a box, bag, or car trunk. When vapor from confined spaces can be directly sampled, the likelihood of detection increases.

Advantages to vapor sampling are that it does not require contact with an object to collect a sample and the sample can be cleaner, which may improve sensor performance. Vapor is the suggested method of detection in cases where it is not possible to make contact with the object that needs to be sampled, or when explosives are suspected of being friction sensitive.

Environmental factors, such as temperature and wind, affect vapor sampling more than swab sampling. Higher temperatures produce more vapor to be sampled. Concentrated “plumes” of vapor will only be present down current or downwind of the target, due to non-uniform mixing of the explosive molecules in the air.

Particulate – Trace particulate residues can be collected from contaminated surfaces using a particulate swipe that is then inserted into the ETD (Figure 3). If a bulk quantity of white powder is suspected as being TATP, it should not be directly sampled. Responders should call the bomb squad and evacuate all personnel to a safe distance.

Particulate screening allows for detection of secondary transfer on personnel and vehicles. Screening is rarely impacted by environmental conditions. Because particulate screening requires contact with the sampled objects, it is not recommended in situations that pose an imminent threat to the screener.

Fluorescence and chemiluminescence based ETDs are capable of detecting trace levels of TATP and hydrogen peroxide, materials that are often used in the manufacture of Homemade Explosive Devices. It can be detected in both particle and vapor modes.



Fig. 3. Particulate-based sample collection and analysis (Source: FLIR, 2018).

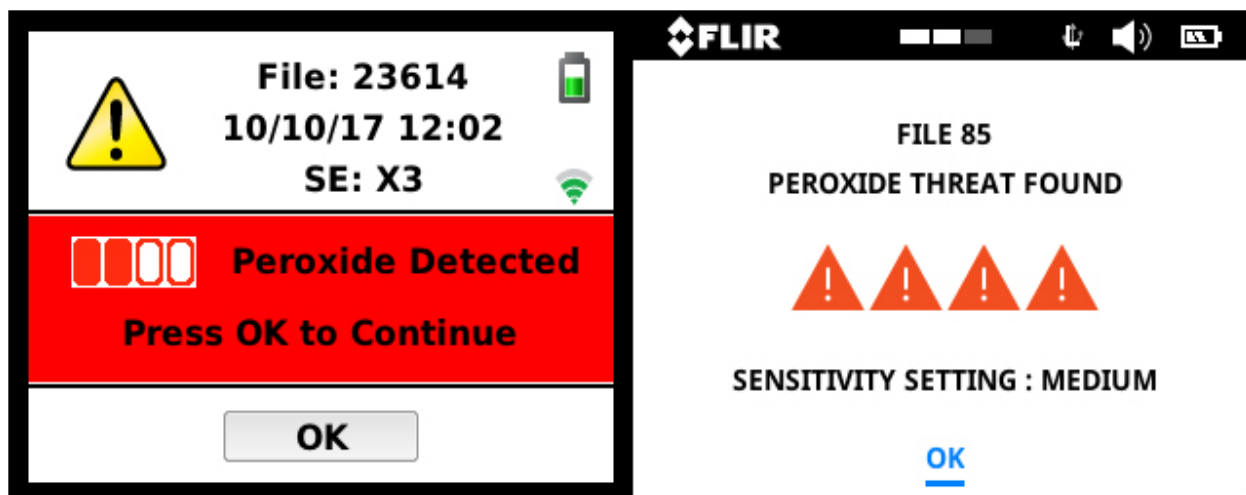


Fig. 4. Peroxide alarm screens on TrueTrace®-based sensor (Source: FLIR, 2018).

Detection of TATP is indicated by audible and onscreen alerts (Figure 4). These ETDs use an open sample flow path, which enables a faster clear-down than other methods, so subsequent screenings can be performed quicker.

Summary

TATP is a common threat used by terrorists, because it can be made from easily available household supplies and produced in makeshift laboratories. This unstable chemical is dangerous to first responders in bulk (visible) quantities. Responders should be aware of the unique signs to look for when TATP manufacturing is suspected and understand that trace (invisible) quantities of TATP can be detected by ETDs using particle (swipe) or vapor sampling methods.

Ryan Holland (pictured above), product manager for explosives and narcotics detection at FLIR Systems, has over 15 years of experience in the development of the Fido X Series sensor (U.S. patent #6,558,626) for detection of ultra-trace levels of explosive vapor and particulates. He has served as a research scientist on a variety of projects related to trace detection of explosives, including landmine detection, improvised explosive device (IED) detection, detection of explosives in marine environments, ageing and chemical transformation of trace explosives residues in the environment, the characterization of explosive chemical signatures associated with IEDs and persons involved in the fabrication of explosive devices, development of forensics tools for use by warfighters in battlefield environments, detection of explosives using canines, and sensor algorithm development.

Dr. Mark Fisher, scientist at FLIR Systems, holds a Ph.D. in physical chemistry from Oklahoma State University. He has been instrumental in the development of the Fido X Series sensor (U.S. patent #6,558,626) for the detection of ultra-trace levels of explosive vapor and particulates. He has served as technical lead on a variety of projects related to trace detection of explosives, including landmine detection, improvised explosive device (IED) detection, detection of explosives in marine environments, ageing and chemical transformation of trace explosives residues in the environment, the characterization of explosive chemical signatures associated with IEDs and persons involved in the fabrication of explosive devices, development of forensics tools for use by warfighters in battlefield environments, detection of explosives using canines, and sensor algorithm development. He has an extensive background in the development of methods and hardware for sampling of trace chemical signatures in gas and condensed phases, including development of noncontact methods for sampling trace particles from surfaces.

Emerging Homeland Security Issues – A 2017 Panel Review

By Joseph J. Leonard Jr.

The 2017 Emerging Homeland Security Issues panel met in December to discuss the current challenges of today's threats, review risk management practices, assess means of strengthening interagency relationships, and to consider future resource requirements.



DomPrep hosted the 2017 Emerging Homeland Security Issues Panel in conjunction with the Clean Gulf Conference in Houston, Texas, on 5 December 2017. The active discussion among panel members and over 80 attendees focused on the developing threat picture, current events, and leveraging technology to meet these emerging threats.

Panel members represented homeland security professionals, including:

- *Lieutenant Commander Dan Crenshaw*, USN (ret.), former Navy SEAL and now candidate for the U.S. Congress from Texas District-2;
- *Steve Kastensmidt*, CEM, CPEA, crisis and emergency manager with the Anadarko Petroleum Corporation;
- *Captain Kevin Oditt*, USCG, commanding officer, USCG Sector Houston-Galveston;
- *Assistant Chief Robert W. Royall, Jr.*, assistant chief-operations, Harris County Fire Marshal's Office;
- *Mark Sloan*, emergency management coordinator, Harris County Office of Homeland Security and Emergency Management, Texas;
- *John Temperilli*, senior consultant with Resilient Risk Management;
- *Steve Weiss*, CMS, CPCU, AMIM, president, Stephen P. Weiss Consultants; and
- *Captain Marcus Woodring*, USCG (ret.), CEM, TEM, chief of Health, Safety, Security, and Emergency Management with the Port of Houston Authority.

Woodring highlighted a key reason for gathering this panel, "As we get farther from 9/11, it is increasingly difficult to do things. "The price of freedom is eternal vigilance." Preparedness specialists around the nation are constantly battling questions of complacency and budget shortfalls, while the current political climate is striving to ensure readiness.

With that said, the panel discussed if the country is as proactive as it needs to be and as proactive as it can be. "We look at a broad spectrum of risks and threats. We tend to chase things as they evolve and then we react to them as a nation," stated Sloan.

That may seem reactive, but the professionals comprising this panel – who are among the most accomplished in each of their fields – are also among the most proactive, especially with regard to homeland security. As Royall said, "Every time we develop a playbook, our

enemies and the folks who don't like us find a way to defeat our play. *INSPIRE* magazine is a great playbook for us to figure out how to defeat them, but as we are trying to figure out how to defeat them, they are studying how to defeat us." This is not a choice, being proactive is necessary to overcome the activities of those who seek to do harm.

The participants discussed an array of issues that keep them awake at night, including:

- Chemical attacks using toxic inhalation hazards materials,
- Innovative ways of conducting biological attacks,
- Vehicle-borne improvised explosive devices and ram attacks,
- Binary devices,
- The ever-expanding opioid epidemic,
- Magnetic car bombs that target individuals,
- Threats to cyber infrastructure,
- Chemical suicides (leading to potential responder exposures),
- Unmanned Aerial Vehicle (UAV) threats (weaponizing and/or swarms or use for intelligence gathering),
- Active shooter scenarios, and
- Other tactics that challenge the imagination.

When these issues are added to a mass gathering scenario – such as a parade, major sporting event, religious or political gathering, or an educational facility's environment – the potential impact of these threats becomes apparent. As Sloan said, "It's the unknown that keeps me up. What is their next tactic? What are they thinking about that we haven't considered yet?"

In the 1700s, Frederick the Great said, "He who defends everything defends nothing." Knowing that everything cannot be protected and that resources cannot be everywhere at once is the foundational concept of risk management. The goal is to do the most possible with limited resources and to protect people and critical infrastructure from adversaries causing irreparable damage.

The panelists mentioned many topics during the discussion, but the following four common themes emerged:

- Building and Sustaining Relationships and Capacity,
- Critical Infrastructure Interdependencies,
- Intelligence Analysis and Information Sharing, and
- Economic Challenges for Leveraging Emerging Technologies.

Building and Sustaining Relationships and Capacity

No organization has the budget to get all the trained personnel, equipment, and facilities needed to meet every safety and security mission that they face in today's all-threat/all-hazard environment. Since 9/11, agencies and organizations have had to build and sustain active and engaged relationships among federal, state, local, tribal, nongovernmental organizations, as

well as the private sector. These relationships enable better pooling of available resources and capabilities to more efficiently and effectively address today's emerging threats.

The Houston-Galveston area is home to the largest petrochemical complex in the Western Hemisphere. Weiss summed up the critical regional relationships:

The key to successful homeland security is active and sustained relationships that enable open and effective communications. The best vehicles for that are the Area Maritime Security Committees and Area Committees in each Captain of the Port Zone. These forums bring together federal, state, local, tribal, and private sector partners to address prevention, preparedness, mitigation, response, and recovery strategies [within the Marine Transportation System]. This is all done ideally before an incident with the goal of preventing an attack or minimizing the impact of an event. They provide great opportunities for networking across the agencies that exercise together, exchange lessons learned and best practices, and address a wide array of issues to keep the marine transportation system safe and secure.

These robust committees with active subcommittees can address a wide array of issues for federal, state, local, tribal, and private sector stakeholders. They look at not only regional strategic issues, but also address the needs of first responders through training, exercises, and available grant programs.

Temperilli agreed, "When the veil of security is breached, the responders are called, so there has to be relationships. We try to address these linkages so that when the veil of security is breached, there are notifications, shared information, and the relationship pieces that help us know what we are getting into." When one looks at the preparedness continuum, it is readily obvious that interagency relationships should be well developed before any incident. More often than not, though, these relationships are not cultivated or maintained in such a way as to ensure long-term benefit. It is incumbent upon preparedness leaders to ensure these relationships are active, dynamic, and sustained, as well as developed within the next generation of preparedness leaders.

Kastensmidt seconded that, "The big take away is relationships. We need to be not only talking to, but talking with, and learning from." This is not a "one and done" activity, but one that requires active involvement by all key agencies and their leaders to be effectively maintained in the long-term.

One way to understand "regional capacity" is to use critical thinking based on prior incidents. Sloan related some local history and failing to appreciate prior shortfalls. Hoping an incident will not happen again and not addressing lessons learned are not helpful. Preparedness leaders need to document gaps and build relationships to help fill them. "During Tropical Storm Allison, we recognized our EOC [emergency operations center] was too small; during Hurricane Ike, we had 525 persons from 119 agencies occupying a 22-seat EOC. If you stood up, you lost your seat. Today, I have 109 seats. During Hurricane Harvey, 935 persons from 140 agencies wanted to play." The key is to identify and document gaps, then keep working on them. "Since 1953, Harris County has averaged a presidentially declared disaster, on average, every nine months, so if you want to practice, you are in the

right location. Use your relationships (federal, state, local, private sector, etc., regardless of location) to help fill your gaps. Be honest with yourself on where those gaps are.”

Royall mentioned capabilities with regards to radiation detection as a good example of some of the challenges associated with capacity building. “Right now, it’s not on the radar screen, being overshadowed by fentanyl, botulinum, bombs in cars. We are doing a good job saturating our environment, the maritime environment, our law enforcement brethren, and our HazMat responders, with lots of radiation detection equipment and decent training. That’s the good news. The bad news is, we don’t have enough.” In preparation for the 2003 Super Bowl, federal, state, and local radiation detection resources were pooled to sweep Reliant Stadium. Teams consisted of a bomb technician, an explosive detection K-9 team, and a third individual with the then-available backpack detectors. That was the readily available and viable means available to ensure safety for the game. It worked. With shortages of trained personnel and resources, there is a continued need for the whole-of-government approach, coupled with support from the private sector, to continue to build and expand the capacity needed to meet emerging threats.

Weiss pointed out that maritime and border security and combating transnational criminal organizations are two other examples of where there is a need for increased capacity, especially since resource shortfalls are making it easier for those seeking to harm the United States and its interests. Almost daily, there are news reports regarding border security and immigration concerns, especially with regard to divergent policies put in place by elected officials. Crenshaw concurred that people at the federal level need to work together on this. In addition, elected officials at all levels of government need to work together to ensure security. He further pointed out that nation states having adversarial relationships with the United States – such as North Korea, Iran, Syria, Russia, and China – “speak the language of realism, and we need people in our government who speak that as well.”

Houston Ship Channel Security District – An unusual entity in this region was formed in 2007 to manage security initiatives within the Houston Ship Channel Region. Oditt pointed out, “This port (Houston) does not wait for government solutions, but what impresses me most is they have the Houston Ship Channel Security District where stakeholders approached the state government and asked to be taxed to facilitate regional security problem solving.” The mission statement of the Houston Ship Channel Security District is:

The Houston Ship Channel Security District will endeavor to provide an integrated strategy to increase the level of security for both the waterside and landside facilities within the District. The goal of the District strategy and services is to increase the preparedness and response to potential security threats by providing reliable, cost effective security systems. The District will promote projects to deter future security threats as identified in ongoing vulnerability and threat assessments. The District will carry out its mission in accordance with Chapter 68 of the Texas Water Code and other applicable laws.

Woodring, who was serving as the deputy sector commander of Sector Houston-Galveston at the time the Houston Ship Channel Security District stood up, stated that, “an interesting model of a funding mechanism designed to support local and regional initiatives ... supported

Harris County Sheriff's Office, Harris County Hazardous Materials Response Team, Houston Police Department, and others. Money is used to support grant requests. It is managed by those entities that are assessed." Here is another model that other port communities around the nation can look at as a model to help enhance relationships and build regional capacity.

Critical Infrastructure Interdependencies

Presidential Policy Directive-21 (PPD-21) identified "[16 critical infrastructure sectors](#) whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." These sectors include:

1. Chemical Sector
2. Commercial Facilities Sector
3. Communications Sector
4. Critical Manufacturing Sector
5. Dams Sector
6. Defense Industrial Base Sector
7. Emergency Services Sector
8. Energy Sector
9. Financial Services Sector
10. Food and Agriculture Sector
11. Government Facilities Sector
12. Healthcare and Public Health Sector
13. Information Technology Sector
14. Nuclear Reactors, Materials, and Waste Sector
15. Transportation Systems Sector
16. Waste and Wastewater Systems Sector

Since Hurricane Katrina, people have learned (and sometimes "relearned" or "failed to learn") how interdependent the nation's critical infrastructure can be.

The Houston-Galveston area is not only home to a vital petrochemical infrastructure, but is the only region in the United States with all 16 sectors. The nation depends on the Houston-Galveston region, and the region depends on each of these 16 sectors to support the nation as a whole.

Since the landfall of Hurricane Katrina in August 2005, preparedness leaders have learned (and sometimes "relearned" or "failed to learn") how much the different sectors that comprise the nation's critical infrastructure depend on one another. Each major natural disaster that has struck since then has reinforced the knowledge that an impact on one of the 16 sectors typically has a negative impact on one or more other sectors, thus further stressing national capabilities and resilience. Oditt commented, "We need to focus on resiliency. However, the biggest challenge we continue to face is complacency." Although the word "resilience" was not widely used 15 years ago, it has become part of everyday vocabulary.

Communications Resilience – The emerging concern here is specifically related to cybersecurity. There are lots of plans on how to prevent an incident, and many others on how to *recover* from an incident, but there seems to be a lack of details on how to *respond* to a cyber incident. Sloan said, “It’s that thing that’s behind everything. How do you protect something that you are not that familiar with? The biggest threat I see is internal.” When someone seeking to do harm already has ready access to IT systems, it can prove difficult to protect them unless significant safeguards are built into systems to ensure resilience.

Oditt agreed that there are “collective gaps in our cybersecurity regime and systems,” adding it is, “unlikely that a cybersecurity incident will affect our physical security. It might affect our access control or monitoring systems, but the reality is that those are things we can mitigate and overcome. The MAERSK cyberattack was a wake-up call and it showed us how companies’ business operations can definitely be impacted globally as well.” The “NotPetya” ransomware attack in June 2017 took advantage of Windows vulnerabilities and threatened data access unless \$300 million in Bitcoin was paid to the perpetrators.

Transportation Systems Resilience – Temperilli compared homeland security efforts for critical infrastructure to a soccer goalie:

No one pays attention until a shot gets thru. We are all goalies trying to plug holes. We engage in a discussion with the industries that manufacture and transport (chemicals) to get their best input as well on the front end to figure out what we can do best and what we can do that makes sense from a cost standpoint. If you raise the regulatory bar exceedingly high or with an unfunded mandate, it falls to the consumers to pay, which can sometimes make the economic engine falter.

Transportations systems throughout the United States are used to some degree by almost the entire population on a daily basis. The immediate impact was seen during major hurricanes such as Katrina, Ike, Sandy, Harvey, Irma, and Maria, with many people both inside and outside the affected areas noticing some impact on their daily lives.

Public Health Resilience – The ongoing and emerging opioid crisis is an example where preparedness leaders need to better assess what this means for homeland security practitioners, how to best approach the crisis as it grows, and how to share valuable information among response stakeholders. Royall specifically highlighted this as one of his most significant concerns when he discussed the current state of affairs regarding this crisis, “We have absolutely forgot everything we learned from the Ebola experience in this country.” Information on potential involvement of opioids needs to be shared from the initial dispatch in order to effectively protect and prepare responders (fire, police, emergency medical services, public health, etc.). In addition, response protocols and resources may need to be pooled and shared to enhance regional capacity, especially if there is a significant increase in calls for assistance.

In addition to the opioid epidemic, Royall also highlighted growing concerns with threat actors using Ebola, as highlighted by chatter picked up by Spanish intelligence along the U.S. southern border. The World Health Organization also fears an upcoming resurgence of Ebola in the coming years. The weaponizing of ricin or botulinum is another growing concern. On

botulinum, Royall said, “There is too much interest about it. Botulinum is the new concern, it’s growing interest in the Middle East with ISIS. It is very easy to produce. I can produce it with some chicken, sunshine, and water and let it decay. Properly used, it can make a lot of people sick. Undetected, it can cause a lot of deaths.” The nation has been fortunate that those seeking to do harm have not been more successful in carrying out a biological attack.

The Ebola crisis of 2014, which began with a single victim in the United States, significantly affected nationwide health networks. A greater number of victims would have overwhelmed them. Resources – such as funding, medicines, training, facilities, etc. – are required to effectively combat potential outbreaks and protect the population. Effective protocols and procedures also much be in place to enable a rapid whole-of-government response; and this response needs to include input from the private sector.

Active Shooter Scenarios – One scenario that seems to touch on almost every critical infrastructure sector is the active shooter scenario. With small arms being the weapon of choice of terrorists – as well as average criminals and deranged individuals – talk of this threat permeates the news cycle. As the vast majority of active shooter scenarios are conducted by either a single individual or a small team, Crenshaw asked, “How do we defend against the new wave of lone-wolf attacks that seem to be the new normal with respect to terrorism?”

Turning facilities into fortresses is neither practical nor desirable, but safeguards are needed to protect workers and visitors. Finding the right balance can be a challenge, but risk mitigation techniques, such as those promulgated by the National Institute of Standards and



Business Resilience Conference

REGISTER NOW AT
www.businessresilienceexpo.org
SAVE \$100
ENTER DISCOUNT CODE
DOMPREP



Technologies can aid preparedness professionals in assessing a wide variety of measures to minimize the impact of an active shooter scenario. Few would argue that more effective and timely background checks on those wishing to purchase small arms would detract from the spirit of the Second Amendment. All panelists agreed that plans should be developed and tested, personnel should be trained in the “Run, Hide, Fight” concept, and first responder agencies should conduct realistic exercises to enhance their preparedness.

Intelligence Analysis and Information Sharing

Without downplaying the importance of gathering information, it is important to understand that, until those details are analyzed by professionals, it is not much more than an accumulation of raw data – sometimes, *a lot* of raw data. Only after effective analysis does information become intelligence that can be used to plan and prepare for incidents and events, respond to potential threats, or strengthen resilience. Even then, this information must be shared with appropriate stakeholders across the whole of government and the private sector in a timely manner. The vast majority of the United States’ critical infrastructure as well as its capabilities are contained within the private sector. As such, the private sector must be a full partner in the development and analysis of intelligence as well as a recipient of appropriate intelligence.

A perfect example of the need for effective information sharing was pointed out by Temperilli with regard to hazardous cargoes such as liquified petroleum gas (LPG), liquified natural gas (LNG), anhydrous ammonia, ammonium nitrate, and chlorine. “We need intel on where it’s carried, how it’s carried, etc. The biggest piece of the puzzle is the brown water fleet [barges along the major rivers that comprise the nation’s inland waterways]. While they know what they carry internally, that information is not shared very well with regulators and responders.” This is something that the Chemical Transportation Advisory Committee is working on at the national level, while the Texas Department of Public Safety Industrial Liaison Officer program performs similar activities at the state level. Other states should consider adopting this model to improve information sharing between the public sector and the private sector.

Economic Challenges for Leveraging Emerging Technologies

The pace of science, research and development, and overall innovation is changing and enhancing the technology used on a daily basis. The pace is so fast at times that many people struggle to keep up with all the improvements in capabilities. Although government is a key player in the development of some of this emerging technology, the vast majority of it actually comes from the private sector. In a manner similar to the analysis of information to make it useful intelligence, the value of emerging technology must be effectively assessed to determine what it can do to improve capacity. To do so requires an investment in personnel and methodologies that can evaluate how effective this technology is, where and when it can be best utilized (as well as where and when it cannot be utilized), and the best means to integrate it in with current capabilities.

Kastensmidt pointed out, “We went to the moon on slide rules and now we have all this technology. And this technology can be used for whatever. It’s the intent for which we use these tools. Technology is moving faster than regulations.” Many look at how to best utilize emerging technology in their homes on a regular basis – for example, cellphones, computers, and televisions. The same should be true at every level of government, “How can

we best utilize available technology that we can afford to enhance our preparedness and/or our resilience?”

Royall reminded participants that there are economic factors in play as well that have to be factored into risk management analysis:

There are concerns about cutting funding that has helped us secure the right kind of equipment and training to respond to and prevent terrorist activities in this country. If that funding goes away, it will be very difficult for our communities to sustain what we already have, because technology is changing so quickly and there are new, nontraditional agents that are emerging in our environment that we have to prepare for. There are only a handful of instruments that we can detect fentanyl with. If you don't have those instruments, you are making an educated guess, betting your life and other people's lives on whether it is or isn't. If not 2% by volume or greater, instruments will not detect – A missed detection can cost people their lives.

Royall stressed the ongoing need to work closely with those in the private sector involved in technological developments to ensure that their products are meeting ongoing needs. He also pointed out that new technology must be field tested by actual users to ensure it meets the current and developing demands.

Woodring agreed on the economic factors, “Balance what you can afford, what is required by law, what is regulated versus what I'd like to have. There is a constant battle to weigh the alternatives. You have to manage security to the threat at hand. Do I have the resources to put into it or do I put that towards making money?” Safety and security risk management enhancements are rarely the means to ensure higher profitability. Security and preparedness managers are challenged with convincing executives (and sometimes shareholders and other stakeholders) to commit greater funds for security enhancements, often at the expense of potential profits.

Royall concurred:

There does have to be a balance. Physical security has come a long way since 9/11. Risk management plans and security plans need to be evergreen documents (with emphasis on sustainment). We all look for better ways to do things and how we can improve the way to do things. We need to be right every time. The bad guys are looking for chinks in our armor, and this is where they are going to pick at it.



Conclusion

This year's distinguished panelists have made it clear that, although Americans in general and homeland safety and security professionals in particular have done much to improve the nation's security posture, intelligence and information sharing, as well as response capacity, a lot can still be done to further enhance the nation's capabilities. As 9/11 gets farther in the past, there has been a drop in funding provided by the federal government to support local initiatives. Port Security Grants that provided \$400 million in 2002 are now funded at only \$100 million. The original cost split started as a 50-50 split between the federal government and the local or private sector recipients and is now at 75-25. With increased contributions required from local governments and private sector entities to obtain grant funding, requests are down.

Crenshaw highlighted the need for national and political will to support these homeland security and national security endeavors. Only in this way can preparedness leaders build and sustain the capabilities needed to keep the nation safe and secure. He pointed out that, "We need people in office who understand these threats with relevant experience dealing with these threats. We need coherent whole-of-government strategies. We all need to get on the same page." And these people need to work together across all levels of government and the private sector to best mitigate the current and emerging threats that communities and the nation face.

Weiss agreed, "It's not just folks at conferences like this, but folks everywhere need to become part of the solution." Perhaps "whole of government" should become "whole of nation."

Kastensmidt also considered the need to address these topics with the next generation in mind, "How do we speak to that next generation? How do we peak their interest to help with homeland security issues?" That is definitely something that homeland security professionals need to address sooner rather than later. The seasoned veterans comprising this panel, as well as their counterparts around the nation need to start mentoring the next generation to develop the same level of drive and determination to achieve exceptional readiness with regard to homeland security and national security.

In closing, Woodring challenged all attendees. "You are all outstanding in your field. You are all professionals. You need to be that lone voice. You need to not forget 9/11. You need to go back to that eternal vigilance." It is incumbent upon all homeland security stakeholders – as individuals, groups, or organizations – to heed this advice from learned professionals and to see what can be done to improve the nation's safety and security over the coming years.

CDR Joseph J. Leonard Jr., USCG (ret.), MEP, MCP, CEM, CHPP, CPE, is a 30-year veteran of the Coast Guard and is a Principal with the Penta Consortium Group. He serves as the chair of the Greater Harris County Local Emergency Planning Committee and actively serves in the U.S. Coast Guard Auxiliary. He holds designations as a Master Exercise Practitioner, Master Continuity Practitioner, Certified Emergency Manager, Certified in Homeland Protection Professional, and Certified Port Executive. He has a BA in History from the Virginia Military Institute and an MS in Engineering Technology from Murray State University.

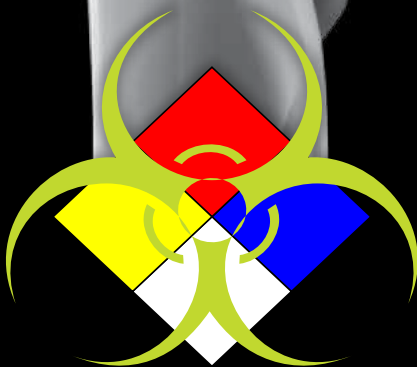
Invisible Threats Exposed



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