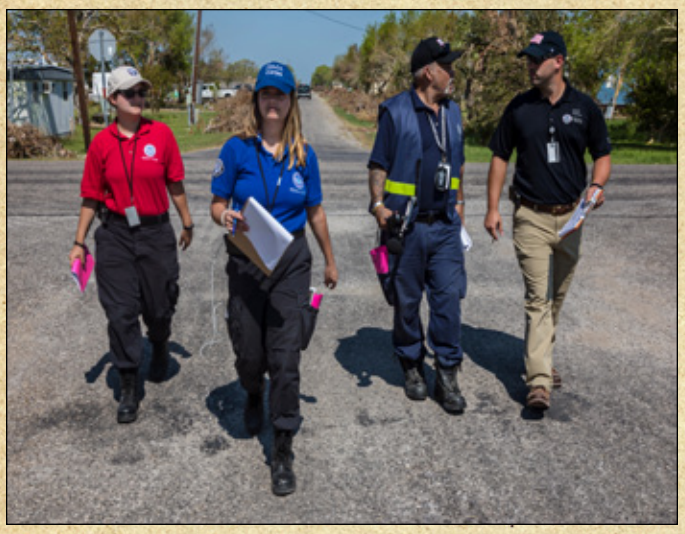
domestic preparedness .com

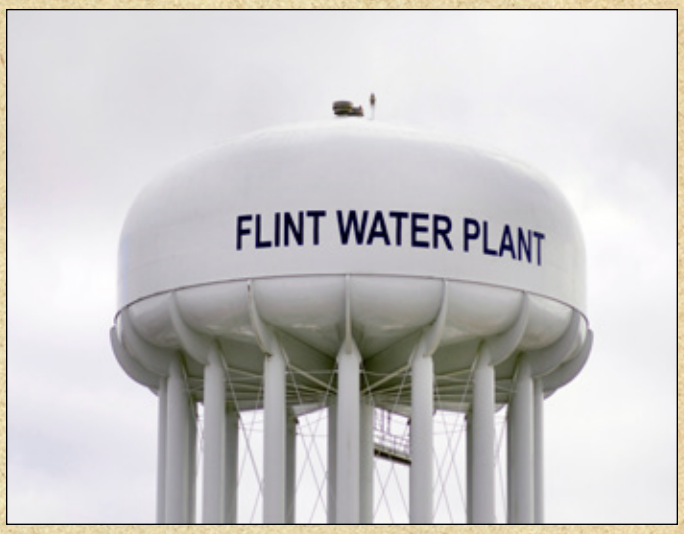
DomPrep Journal

Subscribe

Volume 14, Issue 9, September 2018

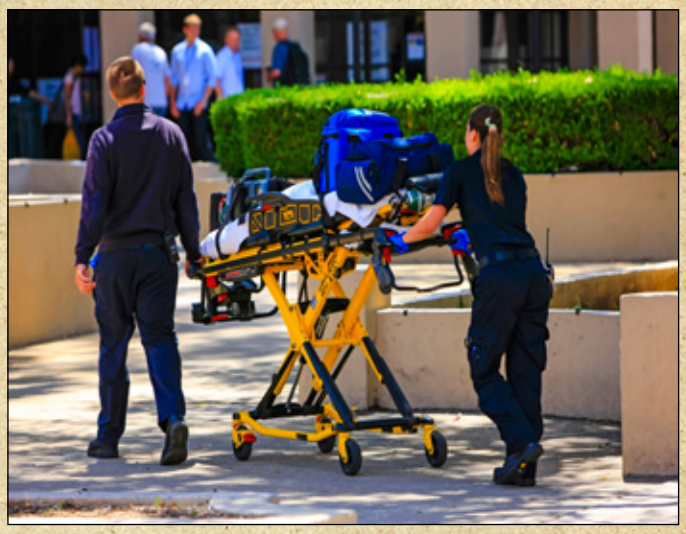


FFEMA Challenges & Responses, 2017-2018
By Kay C. Goss



Introducing the "ACT" Crisis Management Framework
By Terry Hastings

Control System Cybersecurity Concerns
By Joseph Weiss



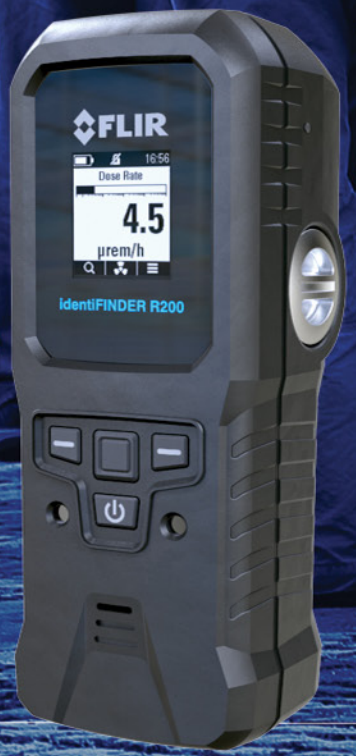
EMS Is EMS – Own It
By Catherine L. Feinman

RADIATION SOURCE IDENTIFIED

Knowing is half the battle. The FLIR identiFINDER® R200 is a rugged, pager-sized Spectroscopic Personal Radiation Detectors (SPRD), that delivers immediate threat alarms to keep you, your team and the community safe. Small, sensitive and effective, the FLIR R200 is perfect for detecting RAD at routine traffic stops, high visibility events and at critical infrastructure entry points.

Learn more at flir.com/R200

FLIR®



FLIR identiFINDER® R200

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

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

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

Carole Parker
Manager, Integrated Media
cparker@domprep.com

Advertisers in This Issue:

BioFire Defense

Environics

FLIR Systems Inc.

PROENGIN Inc.

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

IMR GROUP

Featured in This Issue

Pictured on the Cover: (top row) Goss, Source: FEMA/Christopher Mardorf, 2017; Hastings, Source: ©iStock.com/LindaParton (second row) Weiss, Source: ©iStock.com/metmorworks; Feinman, Source: ©iStock.com/csfotoimages

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!

BIOFIRE®

DEFENSE

Learn more at www.BioFireDefense.com

September – A Busy Month of Preparedness

By Martin Masiuk

September always seems to be a very busy month, not just because it is preparedness month but also considering the large number of meetings, conferences, contract/budget/procurement cycles, and so on. This is true for Team DomPrep too. Two important events happened last week that need to be shared with the readership.

First, on Tuesday, 18 September, DomPrep hosted a roundtable that included 16 subject matter experts. The conversation centered on the "Harmful Risks to Preparedness Professionals From Fentanyl/Opioid Exposure." Important takeaways will appear in a future edition of the DPJ Weekly Brief along with an article on DomesticPreparedness.com.

Second, last week President Donald Trump released the long awaited National Biodefense Strategy and the Memorandum on the Support for National Biodefense. I am honored to report to the readers that DomPrep's policy organization, the Preparedness Leadership Council, is planning to host a roundtable conversation on that strategy in mid-October. I am also privileged to announce that Dr. Robert Kadlec, MD, the Department of Health and Human Services' Assistant Secretary for Preparedness and Response (ASPR) has agreed to be the keynote speaker at this event. We look forward to learning details about the strategy and particularly the ASPR's vision on how to execute it.

DomPrep readers may remember that this topic has been covered in the *DomPrep Journal* in the past. We can only hope that this administration's ability to fund and execute will be different because strategy without funds is just rhetoric. So, we are hopeful that this administration can meet expectations on the five goals they have outlined. The threats, vulnerability, consequences, and interdependencies from a biological event are just too cataclysm to ignore. DomPrep's readers can look for a comprehensive report based on key finding and actionable items captured from the roundtable and published later this year.

Also in this month's issue:

- A former associate FEMA director in charge of national preparedness, training, and exercises addresses how FEMA's new strategic plan may benefit responses to future disasters.
- A senior policy advisor for the New York State Division of Homeland Security and Emergency Services introduces a crisis management framework that operationalizes key concepts during a crisis.
- An expert on control system cybersecurity shares his cybersecurity concerns and suggestions regarding control systems, which are becoming increasingly vulnerable as systems become more complex.
- An emergency medical technician addresses the perceptions and practices that divide the disparate pre-hospital emergency medical services, as well as possible solutions to bridge the gaps.

FEMA Challenges & Responses, 2017-2018

By Kay C. Goss

The overall goal of the Federal Emergency Management Agency (FEMA), emergency management programs, and the profession of emergency management is to have the disaster system be federally supported, state managed, and locally executed. FEMA maintains a delicate and fragile balance between leading and nurturing this enormous system and this exciting profession. At the same time, disasters are becoming more frequent, more intense, and more expensive. Nevertheless, as the U.S. Department of Defense has said it can fight three wars at once, FEMA and its partners could handle three disasters at once. Currently, though, FEMA is clearly faced with handling much more than three major disasters at once.

Current leadership at FEMA was confirmed in June 2017, when the emergency management community and its partners were pleased to welcome a seasoned emergency manager to the helm. It is hard to imagine the nation facing the onslaught of disasters over the past year, without a strong, experienced emergency manager in charge. Emergency management is exceptional in requiring an intergovernmental, interagency, and interdisciplinary process, often termed "the whole community," which includes: federal agencies; states and Washington, DC; tribes; territories; counties; cities; special districts; private sector; nonprofit sector; and the public. Every one of those components looks to the FEMA administrator for leadership, direction, and collaboration, as well as deep emergency management knowledge and experience. In June 2017, FEMA was supporting 692 federally declared disasters.

History

A couple months later, hurricane season hit to an unusual extent, first with Hurricane Harvey in Texas (Category 4), which hovered over Houston for four days. The whole world watched as the city seemed to sink beneath waves of water. Once it became clear that the hurricane was in route to his city, the mayor of Houston decided that the city was too large to evacuate, leaving hundreds of thousands of people sheltering in place. The sustained federal, state, local, and general response phase lasted three months. The recovery phase will last for a decade and more. At the same time, 16 other named storms – including 10 that turned into hurricanes – followed.

FEMA's After Action Report indicates that 80% of those households affected in Texas did not have flood insurance. As a result, there was very little coverage for water damage, but more coverage for wind damage. However, that distinction is often difficult for clients to prove to their insurance companies.

Meanwhile, the future and form of the National Flood Insurance Program was deeply in debt and its future was being – and continues to be – debated by congress and the administration, which has offered/suggested many major changes. Part of the billions in debt have been essentially forgiven and paid by congressional appropriations. However, there was not much time for talk or thought because, about 10 days after Harvey, Hurricane Irma, which was one of the strongest Atlantic hurricanes on record, passed over the U.S. territories, Virgin Islands, and Puerto Rico. It also caused extensive infrastructure damage on St. Thomas and St. John, as well as the Florida Keys. Florida successfully evacuated, creating one of the largest and most successful sheltering missions ever. The Seminole tribal community in Florida was also severely impacted and damaged. In addition to Florida, Alabama, Georgia, North Carolina, South Carolina, and Tennessee were impacted.

At that point, seven states, two U.S. territories, and one tribal community were newly declared disasters, while California wildfires were burning more extensively than ever in history.

Then, on 20 September 2017, Hurricane Maria (Category 5) crossed St. Croix, and then hit Puerto Rico as a Category 4. Maria wiped out Puerto Rico's infrastructure and created a desperate and deadly situation. FEMA had pre-deployed to the island, both to respond to the earlier damage and to be on the scene as soon as possible after Maria hit. However, the 3.7 million residents were without electricity, making communications nearly impossible for a significant time. The longest ever FEMA air mission ensued to provide food and water.

The FEMA administrator initiated a new problem-solving Strategic Plan for FEMA and the profession, and commissioned a robust After Action Report.

Distribution efforts were more challenging than any other disaster in history. During that initial FEMA response, Hurricane Jose also threatened Puerto Rico and the eastern coast of the United States for almost two weeks. As FEMA resources and personnel were required for simultaneous response efforts, sea transport of resources to the Caribbean was also challenging. Then, Hurricane Nate made landfall in Louisiana near the mouth of the Mississippi River.

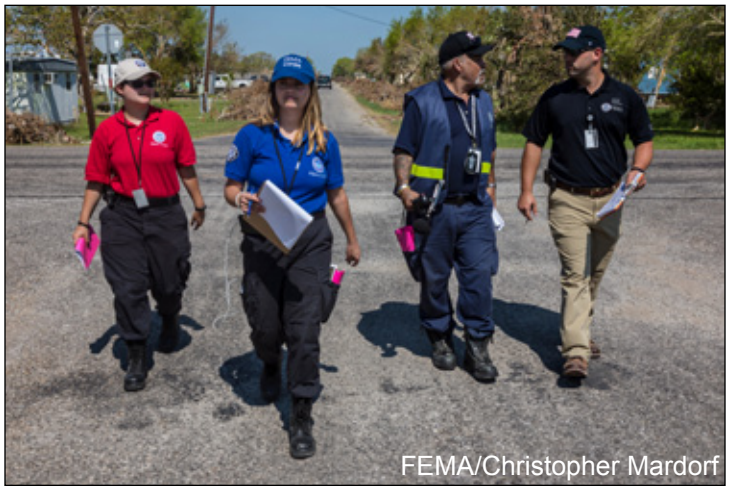
According to FEMA's After Action Report, FEMA delivered 74 million liters of bottles of drinking water, 17 million gallons of water, 63 million meals, and 1,100 power generators to Puerto Rico in the immediate aftermath of the storm. More than $21.2 billion in assistance has been obligated so far. FEMA Urban Search and Rescue Task Forces, with state and local teams of emergency and medical expertise, assisted in the rescue of thousands of disaster victims. Within the first 10 months after the hurricane season, five million applications for disaster assistance had been submitted. Also, the U.S. Department of Defense, the Coast

Guard, state and local managers and responders, nonprofit organizations, the private sector, and neighbors helping neighbors, fleshed out the overall response efforts, led and directed by FEMA.

Nevertheless, there was an extensive number of deaths and overwhelming suffering. Within a couple months, nearly 4.8 million households affected by the 2017 hurricanes and California Wildfires registered for assistance, which was more than the previous 10 years combined.

Lessons Learned & FEMA Strategic Plan

Long-range planning becomes the focus for the future, as well as continuing early stages of recovery, after the initial response. Agencies must learn from the challenges related to these disaster responses and recovery efforts in order to build a better, more robust, system for all phases of emergency management (preparedness, mitigation, response, and recovery), its partners, and its profession. To do so, the FEMA administrator initiated a new problem-solving Strategic Plan for FEMA and the profession, and commissioned a robust After Action Report.


FEMA/Christopher Mardorf

In line with the FEMA overall goal of empowering "A Prepared and Resilient Nation," the Strategic Plan and – in collaboration with states, territories, tribes, cities, counties, special districts, private sector, and nonprofits – a new Strategic Plan was designed and goals were set for FEMA and the profession in 2018-2022. This plan establishes performance measures and highlights its subtitle, "Helping People. Together." This endorses and builds on the teamwork and partnerships that are so crucial to successful emergency management going forward.

1. **To create a culture of preparedness in the country** – This goal is key to a workable process toward achieving resilience. It includes: adding emergency management curriculum in schools (e.g., Head Start programs, pre-K through Ph.D.), more support for higher education and training programs in emergency management, more emphasis and investment in remedial mitigation projects; as well as requirements for initial developments, closing the insurance gap, and learning from every disaster on ways to work together better and to build back stronger. Accreditations such as the Emergency Management Accreditation

Program, standards such as NFPA 1600, and certifications such as IAEM's Certified Emergency Manager® provide support and foundation for many of these processes. The International Association of Emergency Managers (IAEM) and the National Emergency Management Association (NEMA) are key partners in this process, as well as all the other contributors to professional growth and leadership development for the profession. Learning from past disasters will be promoted and shared broadly throughout the profession and its partners.

2. **To reduce the complexity of FEMA processes** – This aspect of the new FEMA Strategic Plan includes streamlining/simplifying the whole process of applying for disaster assistance and grantee experience, as well as maturing the National Disaster Recovery Framework, including Public Assistance project worksheets, and Individual Assistance – including sheltering. This would provide innovative systems for essential flexibility to respond to challenging scenarios that cannot be predicted. This goal also will include data analytics to bolster improved decision making and clarity, empowering FEMA staff to make rapid and effective decisions, and enhancing delivery of the agency mission.
3. **To prepare for catastrophic events** – This includes the streamlining of the currently complex process for disaster assistance applications and building a trained, scalable, and empowered disaster reservist and employee workforce. The administrator is co-locating FEMA employees to several state Departments of Emergency Management and intends to eventually extend this to every state and territory. This will strengthen intergovernmental partnerships, as seen with the first co-location in 2005 after Hurricane Katrina of Bill Carwile (FEMA FCO) and Robert Latham (Mississippi Director of Emergency Management). These new integration teams can help states build capacity and coordination. The difference is that the current rollout of co-location envisions a year-round joint information sharing and joint effort, state by state.

Thus, the new strategic plan postures FEMA and the whole community to be able to provide commodities, equipment, and personnel from all potential and nontraditional sources – both planned and unexpected. It also recognizes the necessary preparedness planning, risk assessments, and hazard mitigation necessary in the pre-disaster period will ensure readiness and resilience in the face of future disasters.

After Action Report

As is the practice after every declared disaster response and every training exercise, an After Action Report was compiled to improve the next response and recovery, including enhanced and robust preparedness and mitigation. FEMA objectively examined its own performance and is driving targeted improvements immediately, including these points, as a sample, of the long list of planned upgrades:

- Enhancing the planning process to make it more usable during operations;
- Using and leveraging capability assessments and exercise findings, especially for Puerto Rico and the U.S. Virgin Islands;
- Revising the National Response Framework to emphasize stabilization of critical lifelines and coordination of critical infrastructure sectors;
- Driving outcome-based recovery through expanded use of the Stafford Act, especially regarding public assistance alternative procedures;
- Building Incident Management Assistance Teams, using the Urban Search and Rescue Task Force capability model;
- Completing a disaster workforce review, increasing certifications, and updating databases;
- Evaluating ways to improve tracking of resource distribution without slowing the process, which includes engaging state® and territorial governments;
- Providing more support to the contracting staff, including pre-event contracting, contract enforcement, and vendor-managed inventory;
- Improving the housing inventory process, including consideration for long-term housing; and
- Promoting all-hazard insurance so individuals can reduce their losses and speed their recovery.

Conclusion

The press coverage of and commentary on these disasters is quite helpful to FEMA, its partners, and the profession of emergency management, in that the public as well as FEMA partners can better understand the efforts, successes, and shortcomings of each disaster. Everyone learns together because the whole community is challenged to care for each other and to build back stronger in the face of inevitable future disasters. The press coverage focuses all stakeholders on the support needed for this vital aspect of local, state, federal, and territorial governments and their multitude of partners.

Kay C. Goss, CEM®, is president of World Disaster Management. She is also part-time faculty online and Go-To-Meeting, as well as in person, in the Executive Master's Program in Crisis and Emergency Management at the University of Nevada at Las Vegas and in the Graduate Program in Emergency Management and Homeland Security at Metropolitan College of New York. Previous positions include: executive in residence at the University of Arkansas; senior principal and senior advisor of emergency management and continuity programs at SRA International (2007-2011); senior advisor of emergency management, homeland security, and business security at Electronic Data Systems (2001-2007); associate Federal Emergency Management Agency director in charge of national preparedness, training, and exercises, appointed by President William Jefferson Clinton and confirmed unanimously by the U.S. Senate (1993-2001); senior assistant to the governor for intergovernmental relations, Governor William Jefferson Clinton (1982-1993); chief deputy state auditor at the Arkansas State Capitol (1981-1982); project director at the Association of Arkansas Counties (1979-1981); research director at the Arkansas State Constitutional Convention, Arkansas State Capitol (1979); project director of the Educational Finance Study Commission, Arkansas General Assembly, Arkansas State Capitol (1977-1979).

Introducing the "ACT" Crisis Management Framework

By Terry Hastings

There is no shortage of crisis management tools and concepts, yet individuals and organizations often still struggle to respond effectively when a crisis occurs. There are likely numerous reasons for this, but one challenge stems from an inability to operationalize the key concepts during a crisis. It can be helpful to establish frameworks that can serve as "mental cues" to organize, guide, and prompt action. This article examines one such framework.

To be effective, a framework must be both intuitive and action oriented because, although it is critical to act quickly during a crisis, it can be difficult to remember and process information during high-stress situations. In simple terms, examples of this kind of quick and easy-to-remember call to action include: "stop, drop, and roll"; "duck and cover"; and "run, hide, fight."

Crisis communicators have long promoted the 27/9/3 concept when it comes to communicating information during a crisis. This means that the communication should be 27 words or less, take no more than nine seconds to convey, and only include three messages. The three-message theory is grounded in the work of psychologist George A. Miller and others who have found that the brain is limited by the amount of information it can process, especially during high-stress situations.

Responsibility, Communication & Opportunity

In addition to serving as an effective means to communicate externally, the 27/9/3 concept can also provide the basis of a framework to help guide the actions necessary to respond to a crisis. To that end, consider the "ACT" crisis management framework, which includes three key actions regarding how individuals and organizations should respond to a crisis:

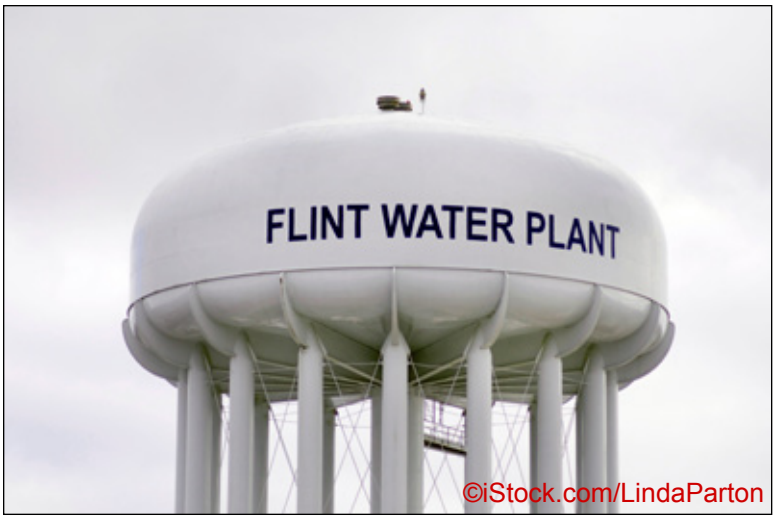
- Accepting responsibility and working to address the problem;
- Communicating quickly and effectively with stakeholders; and
- Taking advantage of the opportunity to learn from the crisis and improve as an individual or organization based on any lessons learned.

Accepting responsibility begins by identifying that a crisis exists; yet, denial (or delay) is too often the first reaction. Whether responding to a disaster or some other type of situation that may threaten the reputation of an individual or organization, time is of the essence. It is critical to accept the situation before it can be dealt with effectively.

The Flint, Michigan water crisis provides an example of what can happen when there is a failure to accept responsibility. In this case, government officials were slow to recognize the situation, which led to more people getting sick and greater long-term damage to the infrastructure. Alternatively, the Tylenol cyanide incident in the 1980s is an example of an organization, Johnson & Johnson in this case, acting quickly to respond to a crisis and to accept responsibility. The company pulled all the Tylenol products off the shelf in what was, at the time, the largest product recall of its kind, plus they fully cooperated with the authorities to investigate the situation. Ultimately, the company's reputation remained intact and they quickly regained the confidence of consumers.

Bad News Does Not Get Better With Age

It is also imperative to communicate quickly and effectively with stakeholders, including the public and others with vested interests in the situation. In today's age of social media and the 24-hour news cycle, it is more important than ever to move quickly to share information. Doing so can help control the narrative and shape public opinion. During a crisis, complete silence is rarely the best option. However, an effective communication strategy would leverage social media and other mechanisms to disseminate the message, ideally using the 27/9/3 concept noted above. Depending on the nature and magnitude of the crisis, the media will likely have a strong desire for information. If they are not getting what they need they will find and tell their own versions of events.



Crisis communicators must also balance the need for speed with the need for accurate information. Again, the Tylenol and Flint incidents serve as good examples. Johnson & Johnson engaged in a proactive effort to share information and cooperate with the media, which included effective messaging from the company's chief executive officer and the establishment of a hotline for consumers and the media to call for the latest information. Alternatively, the officials involved in the Flint water crisis were slow to communicate and did not cooperate with the media, which only served to exacerbate the situation and anger the public.

The "Silver Lining"

Each crisis presents an opportunity to learn and improve. Understanding what went wrong and how to prevent it from happening again is seemingly a simple concept, but it can be difficult to make the behavioral and/or policy changes necessary to prevent another crisis from occurring. However, mature individuals and organizations are willing to learn from their mistakes and take corrective action.

After the Tylenol incident, for example, Johnson & Johnson spearheaded the effort to create tamper-proof packaging for their products, which ultimately led to the passage of a federal law for all over-the-counter drugs. A state investigation into the Flint water crisis has resulted in criminal charges against state and local officials, including manslaughter charges against five individuals for failing to take action when they knew of the dangers to the public. Time will tell if Flint truly learns from this crisis, but other municipalities across the country should pay close attention to what happened in Flint and learn from its mistakes.

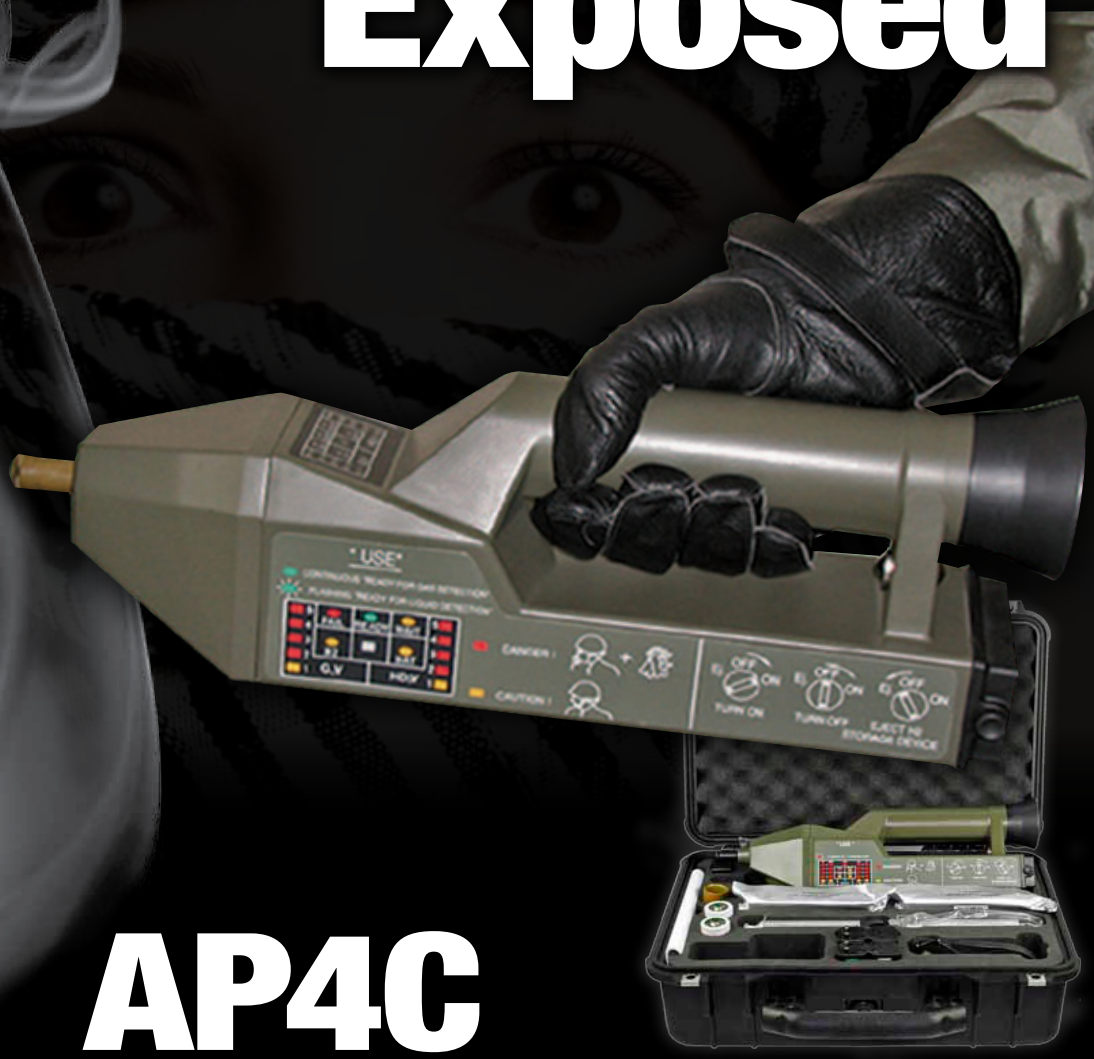
Whether responding to a disaster or some other type of situation that may threaten the reputation of an individual or organization, it is time to ACT.

In addition to the Tylenol incident, the 2013 Boston bombing offers another example of an effective implementation of the ACT framework. First responders, medical workers, and even members of the public accepted responsibility and quickly sprang into action that day to help save lives. The Boston Police Department also did an outstanding job of communicating with the public, to include the use of social media. After the incident, a detailed After Action Report was developed and highlighted areas for improvement. Several officials involved in the Boston bombing attributed the successful response to the lessons learned from prior events and the strong partnerships between the various response agencies.

The ACT framework is not groundbreaking by any means, but the value is in its simplicity and the ability to apply the concept to almost any crisis. In addition to serving as a tool to help improve crisis management, it can also be used as an analytical framework for academics and practitioners to examine how individuals and organizations responded to a crisis. Ideally, the insights gained from this analysis will help others to avoid a crisis all together.

Terry Hastings is the senior policy advisor for the New York State Division of Homeland Security and Emergency Services and an adjunct professor for the College of Emergency Preparedness, Homeland Security and Cybersecurity at the State University of New York at Albany.

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

PROENGIN

Chemical and Biological Detection Systems

Control System Cybersecurity Concerns

By Joseph Weiss

The U.S. electric grid, which was designed more than 100 years ago, consists of control systems and field equipment. The grid was originally designed with large central station generation – for example, coal, oil, nuclear, natural gas, hydro – with transmission and distribution substations to deliver electricity to the end customer. As central station power plants are being supplanted by renewable generation from sources such as solar and wind, control systems are becoming more complex and increasingly vulnerable to cyberthreats, especially as the control system networks are connected to the internet.

The grid has operated effectively, though not necessarily as efficiently as possible, before there were Internet Protocol (IP) networks and Microsoft Windows Human Machine Interfaces (HMIs), which are maybe 15-20 years old. The grid can operate without the internet, but the internet cannot operate without power.

IP networks and associated HMI/SCADA systems provide an extended situational awareness capability, productivity improvement, and capability for controlling various forms of generation. However, they also bring a cybersecurity threat. For many people, grid cybersecurity means preventing a network compromise that can lead to short-term outages of hours to days. Short-term outages from natural disasters and equipment failures were addressed by having redundant systems and equipment spares and by utilizing mutual aid from other utilities when needed. However, mutual aid may not be available after a cyberattack against the grid.

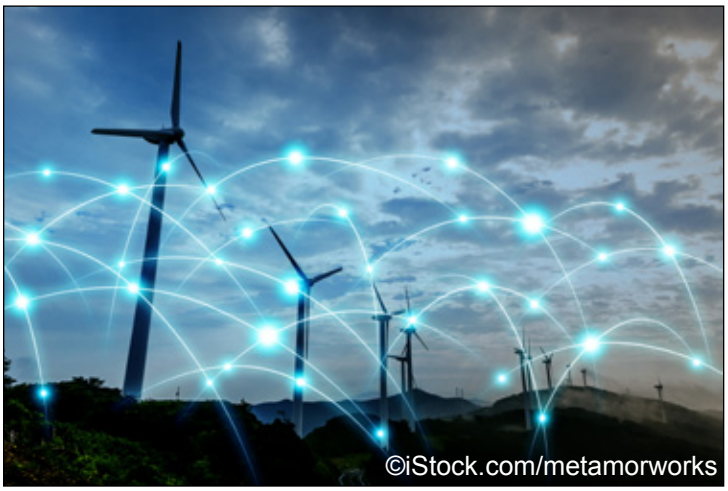
Control System Vulnerabilities

The control systems used to monitor and control power plants and substations do not have adequate cybersecurity, nor do the utilities have adequate control system cybersecurity policies and procedures. Additionally, physical security, IT security, and business continuity policies must be coordinated with control system cybersecurity policies to ensure safe operation and recovery. It should also be noted that concerns about the electric grid also affect chemical plants, pipelines, water systems, manufacturing, and transportation, as these industries all use similar equipment from the same suppliers with the same cyber vulnerabilities.

Control system cyberthreats are important because cyberattacks could physically damage critical equipment (as if from explosives) – such as generators, transformers, and pumps – which can lead to long-term outages (months to years). Damaging this equipment could also lead to injuries to utility personnel and first responders. Control system cyberthreats include network vulnerabilities and engineering system vulnerabilities. Addressing network cyber vulnerabilities is necessary but not sufficient to protect the grid from cyberthreats.

The Aurora hardware demonstration in March 2007 at the Idaho National Laboratory is an example of a cyberattack that does not involve network malware but damages critical substation and other hardware equipment. This type of attack can bring down the grid – as well as any facilities that are connected to the affected substations – for 9 to 18 months. The damage occurs in milliseconds and only specifically designed hardware can prevent it.

The details of the Aurora vulnerability were made public and have been on hacker websites for several years. The 2015 Ukrainian cyberattack was step one of the two steps of Aurora. If the attackers had reclosed the substation breakers they had opened, the outage would not have been 6 hours but 6 months as critical equipment could have been damaged. This level of damage could have been considered an act of war.



Network monitoring, however, can do little to identify these types of attacks. Other cyberattack scenarios that target large, long lead-time equipment such as transformers, motors, and generators can cause long-term damage that, like Aurora, are not network-centric and require electrical engineers rather than network analysts to understand. The lack of cybersecurity and authentication of the process sensors – for example, measurements of pressure, level, flow, temperature, voltage, current – actuators, and drives can directly lead to loss of safety that will not be identified by network monitoring.

Call to Action for Emergency Operations

First responders and recovery operations have well-developed policies, procedures, and training for recovery from major outages generally caused by natural disasters such as earthquakes, floods, and tornadoes, or equipment-caused outages such as the 2003 Northeast Outage. However, cyberthreats can cause issues beyond those caused by natural disasters or equipment failures. Control system cyber events can have the following impacts on first responders and recovery operations:

- Recovery programs can take weeks to months when a cyber-physical system is impacted. This already occurred, in 2004, when a utility's SCADA was compromised by a cyberattack. In that case, SCADA was unavailable for two weeks and it took four man-months to recover (see Protecting Industrial Control Systems from Electronic Threats). Capability for extended manual operation may not be available. However, Ukrainian cyberattack experience

showed that an ability to operate using manual means was essential for months after the cyberattack.

- There is low confidence that early information will be correct and high probability that early information could lead to conflicting statements, retractions, etc., which can translate into a public relations ordeal. Obtaining the root cause could take weeks or even months – possibly unknown during the crisis response to the physical impacts. An example was the 2008 Florida outage when the Department of Homeland Security (DHS) did not understand the actual cause yet was providing its public disclosures that the event was not terrorist-related. Consequently, there is a need to understand what has already occurred to better understand the potential impacts and magnitude of the incidents.
- In most cases, it will be a difficult and lengthy process to prove that an event is a cyberattack and not an unintentional incident. In some cases, such as the 2008 Florida outage, the only difference between the incident being malicious or unintentional was the motivation of the engineer, which cannot be identified by technology. The response to a cyberattack may be different than the response to an unintentional incident, yet decisions must be made with limited information. There is generally little control system cyber forensics or training available. Additionally, attackers might have left footholds in other systems that could take weeks to uncover and cause potential safety threats to first responders and maintenance personnel. Consequently, the crisis management team (CMT) needs control system cyber subject matter experts (SMEs) involved. Additionally, third party expertise is often essential.
- Estimating the recovery effort is harder because of the unique issues associated with cybersecurity. There are few documented control system cyber incidents even though there have been almost 1,100 actual cyber incidents to date. Many of these control system cyber incidents have similar characteristics. A cyberattack requires an understanding of how the traditional recovery effort will be affected by cyber issues, and identification of the appropriate cybersecurity people, technology, and physical resources in addition to the traditional people, technology, and physical resources needed to recover from a non-cyber event.
- Mutual aid is an agreement through which other utilities offer their restoration services after natural disasters strike and cause widespread outages. The unwritten premise is that a natural disaster in one region will not affect other regions so that utilities in the unaffected regions can provide restoration support. There is an assumption that a mutual aid approach for natural disasters can be extended to include cyberattacks. However, the premise of cyber mutual aid is flawed for many reasons:

- What is mutual aid for a cyberattack?
- Is it providing technical resources to identify and remediate the cyberattacks? (This has been unsuccessful for IT networks.)
- Is it providing replacement equipment if transformers, capacitor bank switches, valves, motors, etc. are damaged by cyberattacks?
- What happens if the replacement equipment is damaged by recurring cyberattacks?
- Where will the replacement equipment come from if it is not still manufactured in the United States?
- Will the new equipment coming from "overseas" already be infected?

If a utility in one region suffers a cyberattack against its operational systems, other utilities may be ready to respond with mutual aid. However, if another utility in a different region is cyberattacked the next day, every utility will have all available resources dedicated to protecting themselves because the vulnerabilities that were exploited against one utility can potentially be exploited against other utilities using the same equipment. There is a need to understand what has already occurred to better understand the potential impacts and magnitude of the incidents.

- There is a lack of addressing cyber/reliability interdependencies of control system equipment. Since the same control system equipment are used in multiple industries worldwide, an attack in one industry can have repercussions in other industries and regions. Stuxnet is an example. The same Siemens systems controllers that were compromised in the centrifuges in Iran in 2010 are used in power plants, water systems, railroads, breweries, and even amusement park rides worldwide. Consequently, there is a need to understand what has occurred to control system equipment used by any industry to better understand the potential impacts and magnitude of the incidents that could affect the utilities.

With all this in mind, it is imperative for CMTs, first responders, and recovery teams to understand the unique issues that can occur following control system cyberattacks that affect the equipment used in the grid.

Joseph Weiss, CISM, CRISC, is the managing director of Applied Control Solutions LLC, an International Society of Automation (ISA) fellow, managing director of ISA Control System Cyber Security (ISA99), Institute of Electrical and Electronics Engineers (IEEE) senior member, and registered professional engineer. As an expert on control system cybersecurity, he authored "Protecting Industrial Control Systems From Electronic Threats" and gave a keynote to the National Academy of Science, Engineering, and Medicine. He was also featured in Richard Clarke and R. P. Eddy's book, "Warning – Finding Cassandras to Stop Catastrophes." He has two patents on instrumentation and control systems.

EMS Is EMS – Own It

By Catherine L. Feinman

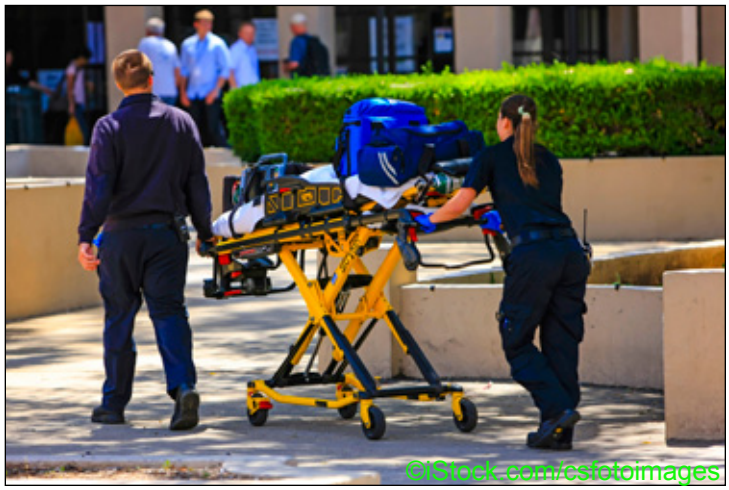
National Preparedness Month is a time for each person to reflect on his or her level of preparedness for the next emergency. This article challenges those in the Emergency Medical Services (EMS) to do the same. Whether training for Basic Life Support (BLS) or progressing to Advanced Life Support (ALS), all EMS personnel are created equal at their respective levels. They must learn the same skill sets and protocols and pass the same certification exams as all other EMS personnel within their jurisdictions. That, however, is where the "equality" ends.

After months of hard work and training, it is time to practice those EMS skills as career emergency responders, volunteers in firehouses, members of private ambulance companies, or other positions where EMS skills are essential. Despite receiving the same training and validating competencies at the local, state, and federal levels, expected standards of care vary depending on duty station and or agencies.

Three Key EMS Paths

Generally, there are three service paths for graduating EMS practitioners: career, volunteer, and transport. Each provides different opportunities to practice the profession. Career emergency responders have the benefit of working in the profession regularly each week. The sheer volume of calls they respond to provide them with a wealth of knowledge and innumerous opportunities for practicing their skills. However, this regularity can lead to complacency and a reduced desire to learn and train beyond required refreshers. They also may have little patience for less experienced volunteers and private EMS members.

Most volunteers may not ride as frequently as career personnel, but they tend to be impassioned and have a sense of community, especially during emergencies. They also comprise a significant portion of emergency and disaster response efforts. For example, volunteers in rural and urban areas comprise approximately 75% and 30%, respectively, of the EMS providers. The passion that volunteers have and their connections to their communities, though, can sometimes obscure their ability to accept outside help and training from career and/or more experienced staff.



EMS personnel in private ambulance companies could serve as first responders or manage nonemergency (short- and long-distance) medical transports, depending on the planning and response structure of the local jurisdiction. These members may still be new to EMS, without any experience yet in responding to emergencies, or may have a background as volunteers or career personnel on the emergency response side. As such, they may require more ongoing training to maintain the same skill level as their first responder counterparts. If providing nonemergency medical transport, these members over time may lose some of the EMS skills they learned due to a lack of practice.

Maintaining Equality in EMS

Depending on the frequency of calls and the type of service provided, EMS skills can wane over time, or never fully develop. At a minimum, all EMS personnel must ensure scene safety and body/substance isolation, obtain vitals, and provide patient care within their scope of practice. However, even these core components are at risk. A volunteer eager to get to the scene may forget to do a visual sweep of the area before entering a home. A nonemergency EMS member may think that the vitals taken two hours before they arrived are adequate. A career person in the 23rd hour of his or her shift may not notice the critical difference between this "sick person" with a stomachache and the five others they had earlier that day.

Each EMS provider must be prepared for the next emergency – from a single patient whose condition worsens to a mass casualty incident.

The type of EMS provider – career, volunteer, or private – is not an indication of a person's skills or knowledge set. There are undoubtedly good and bad EMS providers within each type. However, there needs to be a shift away from the stereotypical perceptions that divide the EMS profession – not just about each other, but about themselves as well. For example, "We just transport," is not an excuse to ignore a patient. A "nonemergency" transport does not mean a patient's condition is "nonemerging." Conditions can rapidly change. In addition, a driver who is trained in EMS is not just a driver. Remember that.

Regardless which type (or types) of EMS position someone holds, it is critical to maintain the level of patient care he or she was trained to perform. "Use it or lose it" has two key meanings for EMS and other emergency preparedness personnel:

- Regular practice is needed to maintain what was learned during trainings.
- Ongoing trainings and learning opportunities – beyond simply the required refreshers – are needed to maintain the most current knowledge, skills, and abilities.

Whether regularly responding to emergencies or not, EMS still means "Emergency Medical Services." Each BLS and ALS provider has a responsibility to be prepared for the next emergency or disaster – from a single patient whose condition suddenly takes a turn for the worse to a mass casualty incident. EMS is EMS, and it is time to own it.

Lessons for All Emergency Preparedness Professions

In today's age of preparedness, it is essential that all prehospital providers maintain a competency in providing emergency care and managing trauma. Whether a public or private, career or volunteer EMS provider, all are obligated to maintain core competencies to ensure delivery of care within their scope of practice. Resources such as the National Highway Traffic Safety Administration and the Health Resources and Services Administration's National EMS Scope of Practice Model offer the following benefits:

- Establish national standards for the minimum psychomotor skills and knowledge for EMS personnel;
- Improve consistency among states' scopes of practice;
- Facilitate reciprocity;
- Improve professional mobility;
- Promote consistency of EMS personnel titles; and
- Improve the name recognition and public understanding of EMS personnel.

This article focuses on EMS, but the lessons apply to anyone who is trained and certified to respond to a critical incident. National Preparedness Month is more than citizens simply having plans and building kits. It is a time for professionals to reflect on their past training and certifications:

- Do I remember everything I previously learned? If not, refresh these skills.
- Has anything changed since I learned it? Read trade publications and communicate constructively with others to find out.
- Am I working like I trained? Lead by example to promote continuity of effort between equally trained and certified personnel.

Although many differences exist between career, volunteer, private, and other EMS organizations with regard to costs, pay scales, and services offered, the level of care available from one BLS/ALS provider to another should not vary: BLS is BLS, and ALS is ALS. Providers have the responsibility of ensuring they maintain the competency expected at their respective EMS licensure levels.

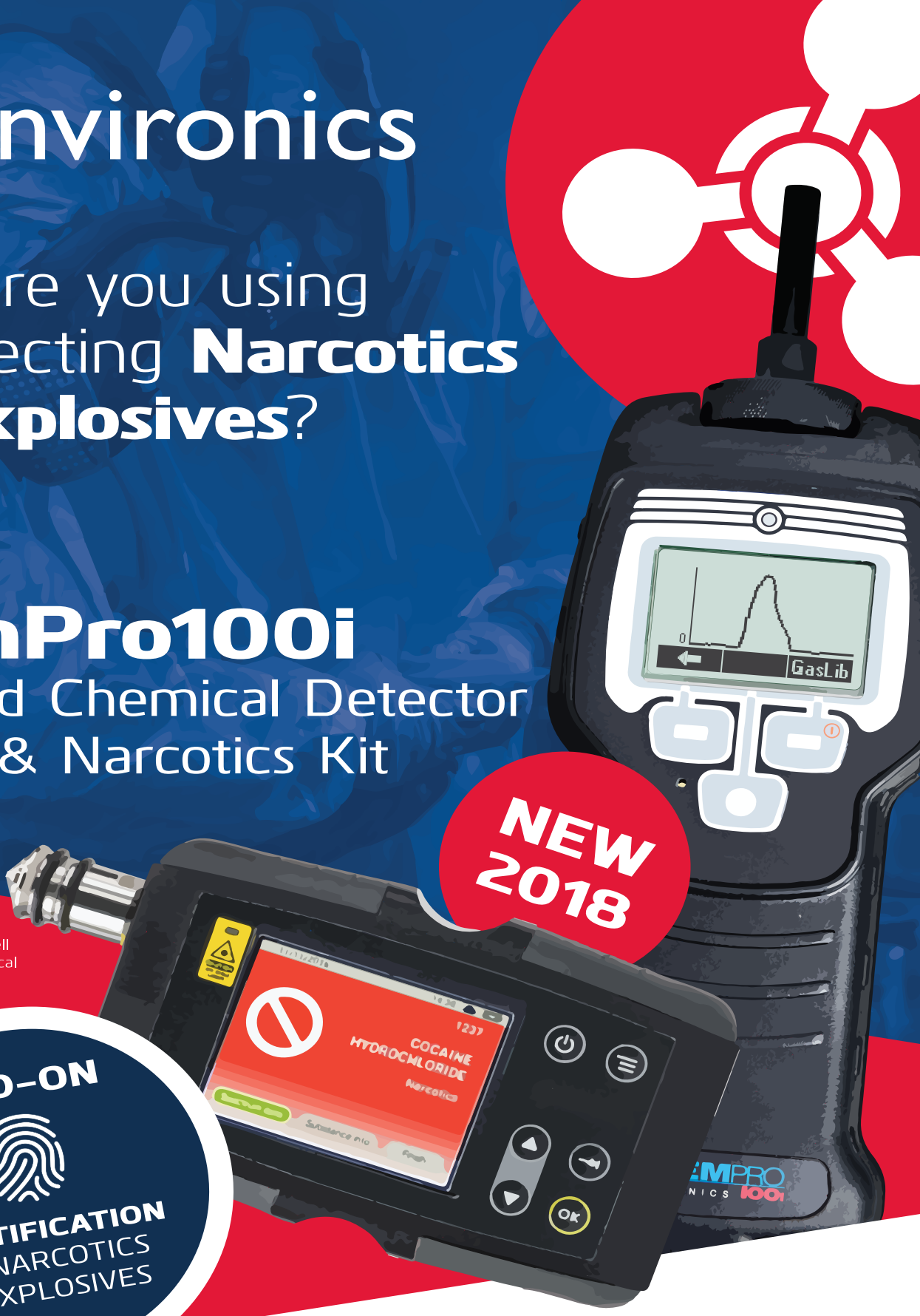
Catherine L. Feinman, M.A., joined Team DomPrep in January 2010. She has more than 30 years of publishing experience and currently serves as editor-in-chief of the DomPrep Journal, www.DomesticPreparedness.com, and the DPJ Weekly Brief. She is an emergency medical technician (EMT) for Hart to Heart Ambulance Transportation. She also volunteers as an EMT/firefighter in Anne Arundel County, Maryland. She is a member of the Media Advisory Panel of EMP SIG (InfraGard National Members Alliance's Electro-Magnetic Pulse Special Interest Group). She received a bachelor's degree in international business from University of Maryland, College Park, and a master's degree in emergency and disaster management from American Military University.

Environics

What are you using for detecting **Narcotics** and **Explosives**?

ChemPro100i

Handheld Chemical Detector CBRNe & Narcotics Kit



NEW 2018

ChemPro100i also serves as a "sniffer" for TICs, Overhaul, Arson, as well as a Biological and Radiological detector when connected to plug-and-play add-on modules.

ADD-ON

IDENTIFICATION OF NARCOTICS & EXPLOSIVES

Welcome to meet us!

Sacramento, CA, September 4th to 7th, 2018

The Continuing Challenge HazMat Workshop Booth 1 joint w/**Gases101**

For further information visit **www.environicsusa.com**