



**The True Test of a Successful
Crisis Response: Public Trust**
By W. Craig Fugate



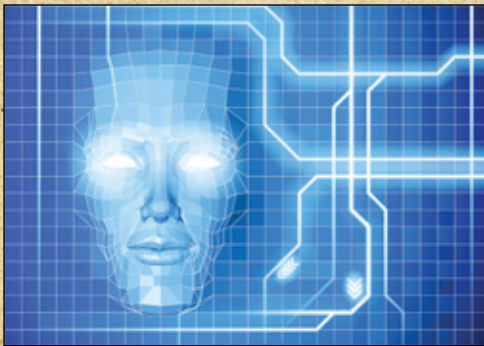
**Anatomy of a National
Special Security Event**
By Christopher T. Geldart



**Why NIMS Continuing
Education Is Needed**
By Randall Hanifen



**Ham Radio in
Emergency Operations**
By Steve Aberle



**Facial Recognition Making an
Appearance in Public Safety**
By Rodrigo (Roddy) Moscoso



**Using Core Capabilities to
Build County Resilience**
By Allen King



**Cuts to U.S. Bioterror Funds
Risk Peril in Event of Attack**
By Daniel M. Gerstein



**Fit for Duty:
The Resilient Responder**
By Anthony S. Mangeri Sr.



NO TIME. NO LAB. NO PROBLEM.

EASILY IDENTIFY CHEMICAL HAZARDS IN EMERGENCY SITUATIONS WITH THE FLIR GRIFFIN™ G510 PORTABLE GC/MS.

Designed for downrange missions, the FLIR Griffin G510 GC/MS features a large touchscreen, long-lasting batteries, and is spray-resistant. Analyzes all phases of matter and confirms vapor-based threats within seconds, so that responders can take immediate, decisive action. To learn more, go to [FLIR.com/G510](https://www.flir.com/G510).



FLIR Griffin™ G510
Hand-Portable GC/MS
Chemical Identifier

Business Office

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

Staff

Martin Masiuk
Founder & Publisher
mmasuk@domprep.com

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

Carole Parker
Manager, Integrated Media
cparker@domprep.com

Advertisers in This Issue:

American Military University

BioFire Defense

Federal Resources

FLIR Systems Inc.

PROENGIN Inc.

© Copyright 2017, 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 Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher.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

Success or Failure of a Response: There Are Options
By Catherine L. Feinman5

The True Test of a Successful Crisis Response: Public Trust
By W. Craig Fugate6

Anatomy of a National Special Security Event
By Christopher T. Geldart8

Why NIMS Continuing Education Is Needed
By Randall Hanifen12

Ham Radio in Emergency Operations
By Steve Aberle15

Facial Recognition Making an Appearance in Public Safety
By Rodrigo (Roddy) Moscoso19

Using Core Capabilities to Build County Resilience
By Allen King22

Cuts to U.S. Bioterror Funds Risk Peril in Event of Attack
By Daniel M. Gerstein25

Fit for Duty: The Resilient Responder
By Anthony S. Mangeri Sr.27

Pictured on the Cover: (top row) Crisis Response, Source: ©iStock.com/annatodica; National Special Security Events, Source: Elijah Crawford, 2017; (second row) National Incident Management System, Source: FEMA/Robert Rose, 2011; Ham Radio, Source: Steve Aberle, 2011; (third row) Facial Recognition Technology, Source: ©iStock.com/ChrisGorgio; County Resilience, Source: ©iStock.com/fairlady; (bottom row) Bioterror Funds, Source: U.S. Department of Homeland Security; Resilient Responder, Source: ©iStock.com/Chalabala.






Introducing HazMatIQ Version 20



- Two New Charts
- Threat Updates
- Faster Response
- Improved PPE Guidance



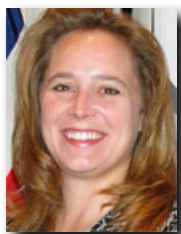
800.892.1099 | www.federalresources.com/training-expertise

 /federalresources
  @fedresources
  /federalresources

Success or Failure of a Response: There Are Options

By Catherine L. Feinman

The success or failure of an emergency response depends on many factors: planning, capabilities, training, tools, funding, public trust, and the list goes on. This edition of the DomPrep Journal examines potential points of failure as well as formulas for success when responding to a crisis.



Of the many different factors contributing to the outcome of an incident's response, the true test for success is the level of trust the public has in emergency managers and responders when a crisis occurs (see [Craig Fugate's](#) article). Decisions surrounding how to prepare, inform, and communicate with the public are critical.

Building resilience from the county to the federal levels requires using local core capabilities. However, in order to effectively leverage these capabilities, guidance is needed to bring new stakeholders such as community associations to the table as force multipliers (see [Allen King's](#) article). Ham radio operators form another key stakeholder community that offers a wealth of knowledge and tools during emergency operations and should be included in comprehensive emergency management plans (see [Steve Aberle's](#) article).

In addition to inclusion of community stakeholders in emergency planning and guidance efforts, continuing education and personal preparedness of responders can determine the success or failure of an incident response. For example, the National Incident Management System (NIMS) and the National Response Framework provide critical guidance for disaster management and response but, without regular refresher trainings, it may be difficult to ensure proper implementation (see [Randall Hanifen's](#) article). The same can be said if responders are not adequately prepared personally with sufficient sleep, diet, and social networks to be ready for duty when needed (see [Anthony Mangeri's](#) article).

Whether preparing for a large-scale event or an emergency incident, having the right knowledge, tools, and funding can make a big difference. Knowing what to expect during a planned event – for example, a National Special Security Event – can help communities take advantage of the opportunities while mitigating the challenges associated with such events (see [Christopher Geldart's](#) article). Having tools to identify threats – for example, facial recognition technologies – can provide public safety professionals with the capability to thwart attacks before they occur (see [Roddy Moscoso's](#) article). Adequately funding facilities and agencies – for example, the National Biodefense Analysis and Countermeasures Center – can sustain much needed knowledge and capabilities to counter efforts of those with the intent to create weapons of mass destruction (see [Daniel Gerstein's](#) article).

The bottom line is that any large-scale event or crisis scenario involves many factors and many decisions. The wrong decisions can be catastrophic, but the right decisions can build resilient communities and reinforce trust among the various stakeholders. Being well informed about threats, hazards, and core capabilities, and being integrally networked within the community, would facilitate the decision-making process.

The True Test of a Successful Crisis Response: Public Trust

By W. Craig Fugate

No organization, or government, can solve every problem. There will always be a crisis that will require an emergency response. And fundamental to the success of that response will be the public's reaction. Emergency managers can react and can mobilize, but they will not be successful unless they do so in such a way as to ensure the public trust. This was apparent in 2005 with Hurricane Katrina, which was a crisis of government.



Emergency managers must approach every crisis considering the following: “How are we ensuring the public maintains its confidence in us?” “Are we maintaining the public trust?” The answers to these questions will be the true test of success.

Be Prepared, Be Credible & Communicate

First and foremost, to help maintain public trust, emergency managers must be prepared to provide a credible, timely response to a crisis. They must be prepared to meet basic needs through responders and perform to the best of their abilities. The path to achieving this is clear, with resources and trainings available to ensure managers can deliver.

But another, equally critical aspect that many emergency managers do not consider or are not comfortable performing is communicating with the public – being honest and transparent to the public, as quickly and as completely as possible. There is this mindset that says, “Don’t tell the public. They’ll panic.” That is not good advice. Transparency is needed

to earn and maintain trust. If senior government officials say one thing, and responders say something different, then distrust is created. And, if people find out they have been misled or purposefully misinformed, that is really bad.

Building public trust is achieved by knowing what to tell the public. First, be clear on the objectives. Let the public know what emergency managers are looking for and what they are looking to do. Then, tell



them in real time what is being done; keep communicating throughout and keep these lines open. And, let them know what is expected of them too. Be concise so everyone understands.

Next, let people know if there will be challenges. Do not say everything is going to be okay when it is not. Do not say there will not be problems, when there will definitely be problems. Be realistic. People must have a realistic understanding of the situation. If something will take days to resolve, tell them it will take days.

A Successful Case of Achieving Public Trust

The Tylenol tragedy of 1982 is a textbook example of how to successfully maintain public trust. Bottles of Tylenol were laced with cyanide, which resulted in several deaths. Johnson & Johnson, the company that makes Tylenol, did not wait for answers: “Was it local?” “Did it come from a lone plant?” They did not know, and they did not care at that point; they pulled ALL their products off the shelf. That was their step one – they provided a credible response.

To test the success of an emergency response, ask the question, “Are we maintaining the public trust?”

Johnson & Johnson also told their customers what they were doing: They told their customers they would not put products back on the shelves until they were sure they were safe.

They communicated throughout the process. They distributed warnings to hospitals and distributors and advertised across national media, warning people not to take any of their products that contained acetaminophen once they determined that these were the capsules that had been affected. The company was clear and concise; they told people what to expect, and they did not “sugar coat” anything.

They also added a critical third piece: they put public safety ahead of their own bottom line. The company did not wait for information or try to minimize the effect on their supply chain. They just pulled all the products. Their reputation was more valuable than anything and, as a direct result, they successfully protected that reputation.

Disasters – Inherently Chaotic

Emergency management is what happens when the traditional organizational chart is no longer capable of managing the crisis. As such, emergency managers must provide a successful response and they must maintain the public’s trust. If the public’s trust is lost, it is not possible to get that time or that credibility back.

W. Craig Fugate is currently senior advisor to the chief executive officer at The Cadmus Group Inc. Previously, he served as the Administrator of the U.S. Federal Emergency Management Agency (FEMA) from May 2008 to January 2017. Prior to his tenure at FEMA, he served as the state of Florida’s emergency management director from 2001 through 2009. In 2016, he received the National Emergency Management Association (NEMA) Lacy E. Suiter Award for lifetime achievements and contributions in the field of emergency management.

Anatomy of a National Special Security Event

By Christopher T. Geldart

There have been 56 National Special Security Events (NSSEs) since Presidential Directive 62 designated the category in 1998, 32 of which have been hosted in Washington, D.C. The most recent NSSEs have been the [2017 Inauguration](#), the [2017 President's Address to the Joint Session of Congress](#), and the [2015 World Meeting of Families](#), which involved a visit to the District by Pope Francis. Local jurisdictions hosting such events must evaluate and plan for both the opportunities and challenges they may face.



Although many communities may never face an event of this scale, there are several, more-common, events that receive federal protection wherein there is a need for federal, state, and local agencies to plan and operate together to ensure the safe conduct of the event. It may include a visit by a high-profile protectee, like the Pope, or situations in which multiple heads of state are attending an event or political rally, like the Democratic and Republican National Conventions. The Secretary of Homeland Security designates an event as an NSSE, at which time the various federal agencies assume the federal coordinating roles for security, crisis management, and consequence management for planning and executing the event. NSSEs differ from other large-scale events in that they have a higher chance of being targeted by terrorism or other criminal activities that may pose a threat to protectees and the mass crowds that often surround these events.

Organization of a National Special Security Event

In accordance with Presidential Policy Directive ([PPD](#)) 15, once an event is designated an NSSE:

- The United States Secret Service ([USSS](#)) is the lead federal agency for coordinating, planning, and security;
- The Federal Bureau of Investigation (FBI) is the lead federal agency for intelligence, law enforcement, and overall “crisis management;” and
- The Federal Emergency Management Agency (FEMA) is the lead federal agency for “consequence management.”

PPD 15 does not supplant the [10th Amendment to the Constitution](#), so the state and in most cases the local jurisdictions still are responsible for the safety, security, response, and recovery for the event. This means that, in cities such as Washington, D.C., or New York City, the local government must plan, coordinate, and acquire all necessary resources for a successful event. It is important for local emergency planners and city officials to understand that these types of events can easily consume the resources of an entire city, so careful planning and budgeting over several months is necessary.

Operations of a National Special Security Event

NSSEs demonstrate a true unified command structure that emphasizes the need for federal, state, and local agencies to work collaboratively during all stages of planning and execution of the NSSE. In the District, the USSS and the District's emergency management have a unique opportunity to physically work together through the Multiagency Coordination ([MAC](#)) center. When possible this entity is co-located with



the District's Emergency Operations Center ([EOC](#)). Operating in the same space has allows all agency's employees to work side-by-side every day, significantly strengthening working relationships and creating a fluid understanding of day-to-day coordination roles.

However, because a lack of capabilities may prevent other jurisdictions from operating this way, it is important to remember the significant challenge of establishing a cohesive [unified command](#). This can often be overwhelming if relationships are not already established and a jurisdiction is new to handling an event of this magnitude. Although the USSS, the FBI, and FEMA descend on a local jurisdiction to organize and secure, the task of security, enforcing laws, and responding to emergencies is the inherent responsibility of the local police and emergency agencies. If an unexpected incident were to happen during an NSSE, it could present a situation where the lead federal agencies shift into support roles, so training for and exercising these scenarios prior to the NSSE is vital to the planning and preparation process.

Resources Required for a National Special Security Event

One of the most important factors for a local jurisdiction to consider when hosting an NSSE is the colossal pull on a city's resources. Depending on its capabilities, handling an NSSE can be all-consuming, and it is easy to lose perspective on the other events or day-to-day operations that require resources. During some NSSEs, jurisdictions may have the ability to shut down much of their daily operations in order to reallocate manpower and minimize the potential for other problems. However, in some cases, this may not be possible. When Pope Francis was in the District, schools were open, businesses were operating, and District agencies had to handle all of it.

The amount of manpower needed for NSSEs should not be underestimated. Local jurisdictions need to investigate what costs may or may not be covered through a federal appropriation for the event. The most successful way to be reimbursed accrued costs is through budgeting before, and accurate cost accounting for time, manpower, and equipment throughout the planning and execution of the event. Local planners should find out what

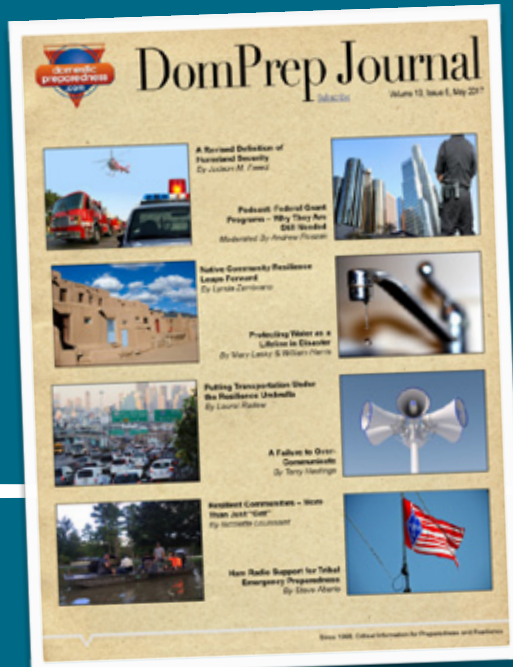
contracts they have in place, for example, with companies that can provide dump trucks to block off streets or buses to be used as safe havens. Jurisdictions have the responsibility for planning for the NSSE in addition to handling the unexpected and continuing to provide its region's basic services. Hosting an NSSE presents the opportunity for a jurisdiction to be challenged as well as to strengthen its preparedness and response efforts in a high-pressure atmosphere.

Christopher T. Geldart is currently the president of C.T. Geldart and Associates. He was the director of the District of Columbia's Homeland Security and Emergency Management Agency (HSEMA) from 2012 to 2017, where he served as the homeland security advisor and emergency manager for the District. He is the former president and chief executive officer of G2 Solutions. Prior to starting G2 Solutions, he was the vice president for homeland security and emergency management for URS Corporation. Before joining URS in February 2009, he was the Federal Emergency Management Agency's (FEMA) director of the National Capital Region Coordination Office (NCRC). Before joining FEMA in April 2007, he worked for the State of Maryland as the assistant director of the Governor's Office of Homeland Security, beginning in 2004. From 2002 to 2004, he was a program manager at Booz Allen Hamilton. From 1989 to 2001, he served in the United States Marine Corps. He has a bachelor's degree in American History from the University of Maryland.

Don't Miss Last Month's Issue!

May 2017

- Homeland Security
- Federal Grant Programs
- Native Communities
- Protecting Water
- Transportation Resilience
- Communication
- Resilient Communities
- Ham Radio



Click to
download now

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



Why NIMS Continuing Education Is Needed

By Randall Hanifen

The National Incident Management System (NIMS) and the National Response Framework are very important and overall well-constructed documents despite some past failures related to their implementation. However, one common denominator in disaster failures or successes is the people involved and the education and training of those personnel. Although federal mandates provide requirements for an initial certification, to date, no required refresher training exists. This article analyzes reasons that the NIMS Incident Command System (ICS) annual recertification should be required to maintain NIMS compliance.



At each level of government, emergency managers and responders have statutory responsibilities related to disasters. Each level of government has certain responsibilities that rely on the actions of other levels. This interconnected aspect of emergency and disaster management allows a failure at any level to compound to a failure at other levels. Hurricane Katrina in 2005 provided a great example of this compounding failure. The [failure of the state of Louisiana](#) was blamed on the Federal Emergency Management Agency's (FEMA) tardiness, and FEMA stated it was awaiting decisions from the state. In 2015, NPR's Maureen Pao described [New Orleans Mayor Ray Nagin's failures](#) to have proper plans in place and execute them in a timely manner, thus creating the extent of the disaster. The disaster declaration process within the United States places the beginning of the response on the local government and, until the local government proves needs beyond their capabilities, the state does not provide assets. This is repeated at the state and federal levels, thus ensuring the management and resources for a disaster are provided by the lowest level of government possible.

Disaster Experience Levels

The federal government response system is made up of career employees that have varying lengths of time in their current positions, political appointees, and disaster assistance employees, as well as the potential for military personnel assigned to specialized Defense Support to Civil Authorities units, such as the Homeland Response Force. Each of these positions has varying lengths of commitment. Although the federal government should be well seasoned in disaster response, FEMA and other disaster agencies at the federal level do not respond in the early hours of an event and are often most associated with recovery efforts. This [changed in the past few years](#) under the direction of then FEMA Administrator Craig Fugate, but the emphasis is still on state and local governments to handle the response at their levels when possible.

At the state level, many career personnel within the state emergency management agency have many years of tenure and, as is the case in many state employment systems, time in grade is one of the biggest deciding factors to promotion. However, in many states, the

state emergency management agency has many areas to oversee and has very few response personnel. In many cases, the response provided by the state is a coordination of other agencies and Intrastate Mutual Aid Compacts (IMAC), which brings emergency managers and responders from different areas of the state. Recently with the enhancements of national qualifications, Emergency Management Assistance Compacts ([EMAC](#)) are becoming more financially feasible for states. This system allows responders from neighboring states to provide response to the affected disaster area.

Local Level & Low Probability

This leaves the local level to provide the majority of the command and control, responders, and emergency management personnel for a [disaster](#). A [2015 article](#), entitled “Comparing Collaboration Between the Fire Department and Emergency Management Agency to the Incident Command System,” found that the probability of a person at the fire department in the state of Ohio serving at a federally declared disaster in his or her current position was 0.0034. Although certain states are more prone to large-scale disasters, the majority of local responders and government officials are in line with this probability. Three factors contribute to this: (a) time in the position; (b) lack of regular disasters; and (c) use of NIMS/ICS outside of the fire department.

First, personnel remain in a certain position within the local government, specifically the fire department for only a few years. As the complete career time in many states is 20-30 years, a person who serves as fire chief for even a few years can only work through the ranks by remaining in any certain rank only a few years. The tasks and needed knowledge to fill positions at the various ranks vary greatly. For example, even if a person were to serve at a disaster as a company officer, his or her role as a fire chief would likely involve participation in the Multiagency Coordination System (MACS), which is an entirely different set of knowledge, skills, and abilities for success.

Second, the low probability of serving in a position at a federally declared disaster is due to a lack of regular disasters. According to FEMA’s disaster declarations, the year 2000 produced three federally [declared disasters in the state of Ohio](#), but a typical year from 2001-2013 is only one or two, and no federal disasters were recorded in Ohio during a few years within that period. This lack of large-scale event experience prevents many of the concepts and structures discussed from the ICS-400 curriculum to be activated on a regular basis. Large-scale structures could be activated for smaller scale events or exercises, but the lack of familiarity tends to shy exercise designers and



Source: FEMA/Robert Rose, 2011

participants away from utilizing MACS, Unified Command, and/or Incident Complexes. Many exercise designers focus more on success of the participants based on their level of knowledge and experience with the NIMS/ICS than to push participants into a non-comfort zone to improve learning. This philosophy is understandable as discouragement can create apathy toward the system and defeat its implementation at lower level events, thus widening the knowledge and experience gap.

Third, although many fire departments utilize a pure NIMS/ICS or some slight variation, this is the only organization within the local government that likely utilizes the system on a regular basis. Because law enforcement officers often operate and arrive solo to events, there

Amount of time in positions, frequency of disasters, and non-fire department use emphasize the need for local agencies to refresh their NIMS/ICS knowledge.

are not many instances to utilize NIMS/ICS. Other divisions and departments within local government do not have any daily use of NIMS/ICS outside of a few examples, such as the United States Park Police and Baltimore Mayor's Office of Emergency Management's use for special events. This creates a great deal of on the spot learning when any

organization besides the fire department needs to utilize NIMS and its terminology. This can lead to communication errors and confusion during the first and most crucial hours of an event unless the local government regularly conducts drills and exercises.

Refresher Training

The partial solution to the lack of use and knowledge retainment of NIMS/ICS is the implementation of an annual recertification course. This could be as simple as a 10-question pretest that adjusts the length of the re-certification course. For example, a correct score on 9 of 10 questions would result in the course only covering the information from the one item missed and increase to a full course depending on the number missed. A pretest would ensure that minimal time would be needed to refresh. This would also allow the after action reports of known issues to drive much of the curriculum.

Although the probability of needing enhanced ICS structures and systems is miniscule, examples show how the lack of competence in NIMS/ICS and the National Response Framework, as well as local disaster plans can have a devastating result that no level of government and resources can overcome. With the laws of the United States comes local control, but also local responsibility. Emergency and disaster management professionals must ensure communities are prepared.

Randall W. Hanifen, Ph.D., is a shift captain for West Chester Fire, an Associate Professor at American Public University, and a public safety consultant. He has a Ph.D. in Homeland Security Leadership and Policy. He is the associate author of the book "Disaster Planning and Control" (2009). He serves as a taskforce leader for a Federal Emergency Management Agency (FEMA) Urban Search and Rescue Team, responding to presidentially declared disasters. He also serves as a planning section chief of a Type 3 Incident Management Team. He frequently writes and teaches on a variety of fire service executive development topics. He can be reached at Randall@Hanifen.org

Ham Radio in Emergency Operations

By Steve Aberle

Many people grew up hearing about disasters in far-off lands and how amateur (ham) radio operators were initially the only means of contact with the outside world. Disasters, both near and far, still occur today, and ham radio operators continue to volunteer their skills and personal radio equipment to serve the public. From a planning and operations perspective, emergency management professionals must effectively include these volunteer resources into comprehensive emergency management plans (CEMPs).



Ham radio was the original electronic “social media” with initial contacts between radio stations taking place in the 1890s. Federal licensing of ham radio stations began after The Radio Act of 1912 was passed, and today all ham radio stations are strictly regulated by the Federal Communications Commission (FCC) under [US 47 CFR §97](#).

The American Radio Relay League ([ARRL](#)), a ham radio member-society founded in 1914, established the Amateur Radio Emergency Service ([ARES](#)) in 1935. This standby radio service consists of “licensed amateur radio operators who have voluntarily registered their qualifications and equipment with their local ARES leadership for communications duty in the public service when disaster strikes.”

In 1952, the Radio Amateur Civil Emergency Service (RACES) was developed as a standby Civil Defense radio service governed by the FCC under [US 47 CFR §97.407](#). RACES is activated by emergency managers in local, county, tribal, and state jurisdictions, uses Federal Emergency Management Agency (FEMA) protocols, and are the only ham radio operators authorized to transmit during declared emergencies when the president of the United States specifically invokes powers granted under [47 U.S.C. §606](#).

Understanding This Communications Resource

Ham radio operators come in all ages and from all lifestyles, and are essentially neighbors in the community. Each licensee has passed one or more extensive knowledge tests covering a multitude of topics, including FCC rules, operator and station license responsibilities, operating procedures and practices, radio propagation, electrical principles and electronic circuits, common transmitter and receiver problems, antenna



Source: Steve Aberle, 2011

measurements and troubleshooting, basic repair and testing, non-voice communications, antennas and feed lines, AC power circuits, and safety.

Since ham radio is their hobby, many hams have decades of radio communications experience. Some may have professional broadcasting experience, and others may be current/former first responders. In standards that have arisen with the introduction of the [National Incident Management System](#), ARES and RACES members may also:

- Be registered emergency/disaster workers under state law;
- Possess certificates for (sometimes many) FEMA training classes;
- Have passed law enforcement background checks; and
- May be engaged in other volunteer activities such as Search and Rescue (SAR) or Community Emergency Response Teams (CERT).

Knowing When/How to Use Ham Radio

The need for supplemental communications increases with incident complexity. If, for example, the incident complexity is [NIMS Type 5 or 4](#), and all communications needs are being handled through commercial services, there is no need for additional communications resources. When incident complexity reaches NIMS Type 3 or 2, regular communications systems may not be capable of normal capacity in the affected areas. Supplemental ham radio communications resources can fill the gap until regular communications are restored. Depending on the quantity of communicators needed and operational periods, deployment of emergency communications resources from outside the affected jurisdiction(s) is possible.

During major emergencies and disasters (NIMS Type 1 incident complexity), there may be major failures and overloading of the communications infrastructure, including the degradation or loss of the electrical grid, cellular phone network, Internet, public safety radio systems, and AM/FM radio systems. In such cases, supplemental emergency communications resources are needed in quantity and for extended periods until regular communications are restored.

FCC regulations permit ham radio operators to serve the public by communicating with non-amateur entities (e.g., FEMA, the National Weather Service, the military) during emergencies and disasters, and when specifically authorized by the civil defense (a.k.a. emergency management) organization for the area served (under RACES protocols):

- 47 CFR §97.111(a)(2) – Essential communication needs and to facilitate relief actions;
- 47 CFR §97.111(a)(3) – With another FCC-regulated service;
- 47 CFR §97.407(d)(1) – Public safety or national defense or security;
- 47 CFR §97.407(d)(2) – Immediate life safety, protection of property, law and order, human suffering/need, combatting of armed attack or sabotage; and
- 47 CFR §97.407(d)(3) – Public information or instructions in civil defense and relief.

In many areas, or with supplemental resources from outside the affected area, ham radio emergency communicators can provide both voice and data communications modes.

Ham radio resources are available for emergency communications support to any public service agency, and can bridge interoperability gaps between served agencies on a local, tribal, and/or state level. Potential ham deployment locations include, but are not limited to, auxiliary command posts, emergency operations centers, emergency shelters, evacuation sites, fire stations, medical facilities, mobile disaster vehicles, police stations, public works sites, and volunteer intake centers. They can also be deployed to provide mobile links to:

- Create communications links between similar agencies across political boundaries, especially where there are misalignments in frequency bands and modes;
- Establish communications in locations outside the existing coverage areas of public service and commercial communications systems;
- “Shadow” critical public officials and emergency management personnel to facilitate constant and rapid contact;
- Monitor crucial infrastructure (such as highways and bridges) and provide periodic situation reports; and
- Staff observation posts (river levels, flooding, damaged areas) and provide periodic situation reports.

While it is unlikely that ham radio will be able to replace all existing communications, the forte of this pool of volunteers is establishing critical communications under less-than-optimal conditions. For hams with solar-powered equipment, they can keep communications going well beyond the limitations of fuel reserves for motor-driven generators until the commercial infrastructure is restored.

Integrating Ham Radio Into the Emergency Management Community

We get so sophisticated and we have gotten so used to the reliability and resilience in our wireless and wired and our broadcast industry and all of our public safety communications, that we can never fathom that they'll fail. They do. They have. They will. I think a strong Amateur Radio community [needs to be] plugged into these plans.

—Craig Fugate, FEMA Administrator (2009-2017), [3 May 2011](#)

As a communications provider, ham radio falls under the [Emergency Support Function #2](#) umbrella. Planning for a “when all else fails” communications scenario is essential for all jurisdictions, and there are multiple ways of achieving this goal at the state, tribal, and local levels. Following are two examples:

- Colorado enacted [HB16-1040](#) in 2016 and put emergency communications provided via amateur radio into public law by establishing an Auxiliary Emergency Communications Unit within the state’s Office of Emergency Management.

- The [CEMP for Clark County, Washington](#), includes the paragraph:

Routine communications systems will be used to the greatest extent possible. When routine communication systems are ineffective, alternate methods, such as amateur radio, will be used to communicate between the EOC, field operations, mass care facilities, and the state emergency operations center (EOC).

As a side note, in late 2015, the emergency manager in Clark County hosted a ham radio license class for his staff, and all emergency management personnel are now licensed ham radio operators.

The old adage about avoiding the exchange of business cards in the midst of an incident is the guidepost here. Each state has one or more ARRL member-elected volunteers who can put emergency management professionals in touch with local hams. So, if a jurisdiction has not yet established an ongoing working relationship with hams in the community, the [section manager](#) listed on the ARRL website can direct these professionals to local ham radio resources.

It is difficult to maintain a cadre of active ham radio emergency communicators in areas that experience little actual activation of those volunteers. To overcome this, frequent involvement in drills and exercises is essential. The professionals need to feel comfortable working with the hams and vice versa. Not every exercise plan needs to include a communications outage in the scenario, but there is no reason messaging cannot take place in parallel by sending the same message over routine communications systems and also via ham radio.



Source: Steve Aberle, 2012

Hams typically like to implement different technologies, so what is transmitted by voice in one exercise might go by digital mode (computer to computer connected to radios) the next, a video link after that, and maybe even via a ham radio satellite at some point. Therefore, give the hams a communications problem and see what they come up with for a solution. Do not dictate the way they should solve the problem, but rather the emergency communications needs requirements. And, make it interesting for the volunteers to keep them involved, because hams could be critical communications lifelines in disasters.

Steve Aberle is a FCC-licensed ham radio operator and been active in the Amateur Radio Emergency Service (ARES) since 1976 and in Radio Amateur Civil Emergency Service (RACES) since 1979. He has served as an ARRL Official Emergency Station in the State of Washington since 1999, and his radio station at home operates on solar power. During his multifaceted career, he was a trooper with the Oregon State Police, a county emergency communications director, a data network manger, and a cybersecurity consultant. He has over four decades of experience in volunteer emergency communications planning, training, responses, mentoring, and exercise evaluation, and is a former mountaineering and Search and Rescue leader and instructor.

Facial Recognition Making an Appearance in Public Safety

By Rodrigo (Roddy) Moscoso

The use of facial recognition (FR) technologies to support public safety has long been considered a potent tool for law enforcement. The capability to automatically identify persons of interest in real-time has the potential to alert police of threats before an incident occurs. Long considered a technology of science fiction, FR is finally moving into the public safety mainstream with new capabilities now being rolled out.



Coupled with “big data” analytics, real-time FR could, for example, monitor the movement of known suspects at specific times and locations, which could then trigger an alert to law enforcement that a potential threat is underway. This includes a known suspect who has arrived at a sporting event or concert venue at an unusual time, or who may be loitering in a location that is potentially vulnerable to the public. The U.S. Customs and Border Protection Agency (CBP) and private sector organizations are finding more ways to leverage this expanding technology.

Protection in the Air

On 2 June 2017, the CBP announced the [rollout of a FR biometric “exit” solution](#) that monitors airline passengers who are leaving the United States en route to Dubai, United Arab Emirates, at Dulles International Airport, which is located near Washington, D.C. Based on the flight’s manifest, CBP automatically creates a set of photos for each passenger from the passport picture as well as other sources, including photos taken during the passenger’s entry into the United States. During the new exit process, a live photo is taken of each passenger and then immediately compared to the existing gallery of photos.

This comparison is designed to ensure that the passenger photographed is the legitimate owner of the travel documents, including the passport being used at that time. Any discrepancy found through the FR comparison would warrant intervention by CBP to confirm that the identity of the passenger matches the documentation. In the 2 June 2017 press release, Acting CBP Commissioner Kevin McAleenan stated that, “CBP has been working closely with airline and airport stakeholders to test biometric exit technology and as a result has developed a viable exit solution based on facial recognition,” and that this process, “enhances our security while continuing to facilitate legitimate travel.”

The use of FR technology will likely raise some privacy concerns for the travelling public. As part of its solution, CBP has integrated the capability to determine if the recognized individual is a U.S. passport holder and, if so, will automatically discard the photo, “after a short period of time.” This may alleviate the fears of some travellers, though others may find the use of this technology unsettling.

As part of an effort to use FR to streamline the boarding process for travellers, the CBP has also partnered with JetBlue Airlines to begin testing a new “self-boarding” process that does not require the use of a physical boarding pass. Instead, passengers who opt in to use

the new solution will have their photos taken and allow the FR system to confirm their identities and allow entry onto airplanes. Initially being rolled out in June 2017 on specific flights out of Boston's Logan International Airport, other similar airline-led pilot programs will be implemented in the coming months.

Protection on the Ground

Beyond the CBP pilot programs taking place today, other FR solutions are being implemented that take advantage of the power of cloud computing. For example, Amazon Web Services' (AWS) FR "[Rekognition](#)" offering is enabling law enforcement entities to leverage their own photo libraries to help identify criminal suspects. By utilizing the technical capabilities of AWS, even smaller agencies can have access to the robust computing power necessary to ensure accurate FR.

Facial recognition is being used in new ways by local and federal law enforcement agencies to ensure public safety on land and in the air.

The Washington County (Oregon) Sheriff's Office is now using Rekognition in an attempt to match images of suspects to known criminals from their own mug shot photos. After

copying all mug shots to the cloud-based program, sheriff deputies can quickly compare suspects to their new cloud-based repository using the computing power that AWS provides. To date, the solution has demonstrated impressive results.

"About 75% of the time, the person we're looking for is identified," said Chris Adzima, senior information systems analyst for the Washington County Sheriff's Office during a phone interview on 23 June 2017. Adzima noted that it took a few days to copy the 300,000 mug shots from the county system, but that the responses to inquiries takes only a few seconds. "It was very inexpensive to implement, and our approximately 20,000 calls to the system each month costs us only a few dollars," he continued.

Adzima added that the source images he receives are often not of good quality – for example, a smartphone picture of a still from a security camera taken off an old cathode ray tube (CRT) monitor. This often requires that he manipulate the image to ensure that the software performs as well as possible, and can include adding facial features to ensure that a nose or the eyes are properly recognized.

Although the advent of real-time FR of large crowds that are then instantly compared to millions of images may still be a ways off, significant strides are being done now to leverage the technology already in place, and at a very low cost. With these elements in place and coupled with talented young technical professionals currently in the public safety space, the future will arrive sooner than anyone may think.

Rodrigo (Roddy) Moscoso is the executive director of the Capital Wireless Information Net (CapWIN) Program at the University of Maryland, which provides software and mission-critical data access services to first responders in and across dozens of jurisdictions, disciplines, and levels of government. Formerly with IBM Business Consulting Services, he has more than 20 years of experience supporting large-scale implementation projects for information technology, and extensive experience in several related fields such as change management, business process reengineering, human resources, and communications.

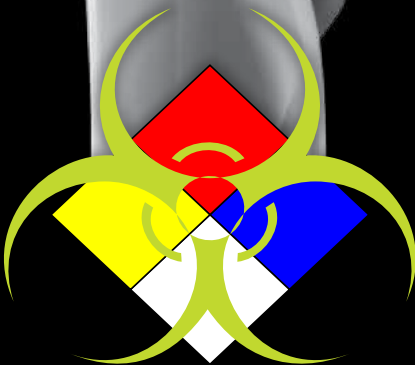
Invisible Threats Exposed



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

Using Core Capabilities to Build County Resilience

By Allen King

The lack of core capability guidance diminishes counties' levels of preparedness and resilience and is a barrier to increasing these efforts for the nation as a whole. By using community associations as force multipliers, counties can leverage this valuable resource to increase resilience-building efforts beginning at the local level. This bottom-up approach builds not only physical but social resilience at all levels.



The stated intent of the core capabilities from the [National Preparedness Goal](#) is to increase the resilience and security of the nation. The [Protection](#) and [Mitigation](#) frameworks describe steady-state actions for protecting infrastructure and systems, and actions to mitigate or protect against the impact that can result from a disaster. The Mitigation framework makes the distinction that mitigation capabilities build resilience and support recovery capabilities.

In the United States, there are [3,143 counties](#), which include county equivalents such as the Louisiana parishes, independent cities in Virginia, Alaskan boroughs, and the District of Columbia. A significant amount of literature is available describing resilience and the core capabilities, but there is inconsistent guidance provided specifically for how a county can use the core capabilities to improve its resilience. Currently, counties have to become familiar with dozens of guidance documents as well as multiple standards. With appropriate guidance and support, counties and county equivalents can exponentially build and improve the security, protection, preparedness, and resilience of the United States.

Built on Security, Protection, and Preparedness

The term “resilience” is often used too casually, with an indifference to changing meanings between mission areas and disciplines. This term can have an active or passive connotation – as tactics or actions used to build or improve communities or as the outcome or result of specific actions, respectively. Resilience can also be described as having both [social and physical outcomes](#).

The core capabilities that add value beyond securing, protecting, and preparing to respond can build resilience for a county. Many of the actions to build and improve resilience are based on mitigation or protection actions for structural, natural, or social forms of resilience. Counties should not limit accomplishing the mitigation core capabilities to only hazard mitigation grant programs. Counties that identify their threats and hazards and complete resilience assessments can reduce their vulnerabilities by mitigation and protection actions for infrastructure systems, the economy, health and social systems, housing, and natural and cultural resources. Improving cybersecurity and the supply chain integrity and security also improve resilience.

Counties should consider developing indicators and [measures for building resilience](#). Although measurement tools do not improve resilience, they can inform the development of strategies to increase efforts. The process of identifying indicators can then determine or confirm what to improve. As such, a county should not limit consideration of actions to meet a resilience target based on a definition, but instead think outside the box, especially when searching for low-cost administrative solutions.

Counties ought to consider modifying the taxation system for homeowners to receive tax credits as incentives for resilience-improving mitigation actions they complete. Counties can also offer an award for exceeding the local building code standard, [negotiate insurance premium reductions](#) for resilience-improving investments, and coordinate for grants, lower interest loans, and [improved bond ratings](#) as incentives for resilience-building improvements.

Community Associations as a Force Multiplier

There are more than 338,000 community associations within the United States. The term community association includes homeowners associations (HOAs), cooperatives, and condominiums. [Community association membership](#) represented about 21.1% of the U.S. population in 2015. However, current volunteer structures do not adequately support the unaffiliated spontaneous volunteer response. [Subject matter experts](#) advocate integrating spontaneous volunteers into disaster planning as force multipliers. A system designed based on the Incident Command System can help counties begin to integrate spontaneous responders within their HOAs.

With more than 338,000 community associations in the United States, counties should leverage these resources as force multipliers to build resilience.

The Bollinger Hills HOA provides an example of a [HOA-based Community Emergency Response Team \(CERT\)](#). The volunteers come from residents within the subdivision trained in CERT curriculum by the Danville and San Ramon, California, first responders. The CERT training is provided during 3.5-hour classes, one night per week for six weeks. The Bollinger Hills HOA also participates in the shorter overview Personal Emergency Preparedness (PEP) training sponsored by the state of California.

The City of Fremont, California, also provides the three-hour [PEP training](#), which includes: an overview of home disaster preparedness, basic fire safety, knowledge of how to safeguard and turn off utilities, an overview of hazardous material, and an overview of weapons of mass destruction. The PEP training also meets the volunteer hours required for high school students to graduate in California.

Counties can promote resilience-building preparedness by implementing the National Weather Service's [StormReady®](#) and the National Fire Protection Association's [Firewise](#)

[USA™](#) programs. At the individual and community levels, promoting individual and family plans and risk-appropriate insurance is important. HOAs then can be used as force multipliers. Counties that use the StormReady© preparedness actions increase resilience by executing the [following actions](#):

- Having a county emergency operations center;
- Possessing multiple ways to receive weather reports and send alerts;
- Having a network of local weather spotters;
- Promoting preparedness; and
- Training and exercising for hazardous weather.

A Resilience Dividend

In her book, [The Resilience Dividend](#), Judith Rodin advocates developing and enhancing a sense of commitment, shared values, and a common identity she describes as “social cohesion.” Strengthening infrastructure and systems is fundamental for building resilience, but a critical component for a resilient county is to build social cohesion. Counties that reduce



the risks and hazard vulnerabilities by improving building codes and zoning, providing incentives for owning a home, and successfully reducing the insurance rates for flood insurance move toward a resilient county. Energizing county residents and businesses to plan together and execute a shared vision is critical. When a county invests in building resilience, it is not only able to respond and recover faster, it can gain new opportunities and become more attractive for new business investments and population growth.

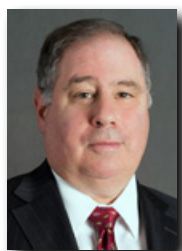
This article is based on the author’s masters thesis, which can be accessed in full [here](#).

Allen B. King III, CEM, is a recent graduate of American Military University (AMU), completing a masters program in Emergency and Disaster Management – with honors. He is an emergency management specialist with the Federal Emergency Management Agency (FEMA), developing doctrinal policy and guidance. He is a retired Army officer with over 34 years of experience in emergency and disaster management. For the past six years, he has taught the Boy Scout of America Emergency Preparedness merit badge to scouts in northern Virginia. He serves as the vice president of the Order of Sword and Shield Honor Society for AMU and is a member of the Delta Epsilon Tau and Golden Key honor societies.

Cuts to U.S. Bioterror Funds Risk Peril in Event of Attack

By Daniel M. Gerstein

President Donald Trump's proposed fiscal year [2018 budget](#) would eliminate a Department of Homeland Security laboratory dedicated to countering bioterrorism and providing the science behind response and recovery efforts should an attack occur. The proposal to eliminate this lab without creating replacement capabilities elsewhere could place the U.S. at risk at a time when biotechnology proliferation is increasing access to the knowledge and capabilities for developing bioterror weapons.



To further emphasize this point, consider that Bill Gates – [who has given billions of dollars to global public health causes](#) – recently said a bioterror attack could [“wipe out 30 million people” and such an attack is becoming more likely](#). The president’s proposed budget, if it were to be adopted by Congress, would zero out funding for the National Biodefense Analysis and Countermeasures Center (NBACC) at Fort Detrick, halting all science as of March 2018 and closing the facility by September 2018. [NBACC was created in the aftermath of the anthrax attacks of October and November 2001](#), which sickened 22 people, five of whom died, and caused some 30,000 people exposed to the highly pathogenic anthrax to begin a regimen of high strength antibiotics. It also required the decontamination of several office buildings and postal handling facilities at a cost of approximately \$320 million.

Following the anthrax attacks, shortfalls in the nation’s bioterrorism preparedness and response capabilities became clearer. The U.S. lacked the facilities, procedures, and people to examine threats at the intersection of terrorism and biotechnology and to conduct forensics in the event of a biological attack.

This threat characterization capability allows operators, law enforcement, public health, and decision-makers to understand the risk of a bioterror attack and the preparedness and response capabilities that should be developed. It also provides a scientific rationale for determining what equipment and medical countermeasures are stored in the [strategic national stockpile](#) maintained by the Centers for Disease Control and Prevention.

The NBACC’s scientists also are capable of conducting experiments to



determine what level of concern is warranted if a potential threat is identified. The NBACC also has bioforensics analysis capabilities. This provides the ability to understand how and potentially where a pathogen was prepared, its virulence and physical characteristics, and even what medical countermeasures and decontamination techniques might be the most effective. Much of the forensics work is done on behalf of the FBI, with the NBACC's experts prepared to maintain chain of custody for samples and testify in court against bioterror suspects.

[NBACC remains a one-of-a-kind facility](#) that provides the U.S. an insurance policy. Its work can help determine how a variety of actors, from lone wolf terrorists to well-financed terror cells, could develop and deploy biological weapons against American targets. It allows experts

to work in the highest containment laboratories with the most dangerous pathogens to protect the nation from a strategic threat, one that some have called "[the poor man's atomic bomb.](#)"

Closing the National Biodefense Analysis and Countermeasures Center would leave the nation without critical capabilities that no other facility can fulfill.

The proliferation of biotechnology coupled with the increasing use of technology by terrorists suggests a growing likelihood of a bioterrorist

attack. Al-Qaida, in a previous version of its Inspire magazine, had called for like-minded scientists – biologists and chemists – to conduct attacks. More recently, the Islamic State group has called for attacks using available means. The degree to which the U.S. will be prepared to respond could be directly related to the preparations made now at NBACC.

Closing NBACC would leave the nation without these critical capabilities. No other such facility exists anywhere in the United States. It was established based on what the government determined to be a critical operational need. It is maintained at significant cost and, like most insurance policies, these costs may not be universally perceived as good investments until they might be needed in a crisis. In the event of a bioterror attack, NBACC would be on the front lines, providing essential information that would inform decision-makers and save lives.

The initial proposal to zero out the capabilities currently invested in NBACC would seem at the very least worth a second look by policymakers. They should assess whether NBACC's capabilities, as an insurance policy, is a price worth paying when weighed against the potential cost in human terms of even a limited bioterror attack.

This article was originally published in "[The Hill](#)" on 6 June 2017. It was reprinted with permission.

Daniel M. Gerstein works at the RAND Corporation and is an adjunct professor at American University. He was the undersecretary (acting) and deputy undersecretary in the Science and Technology Directorate of the Department of Homeland Security from 2011-2014. Gerstein oversaw the National Biodefense Analysis and Countermeasures Center (NBACC) during his time at the U.S. Department of Homeland Security.

Fit for Duty: The Resilient Responder

By Anthony S. Mangeri Sr.

The term “fit for duty” in modern firefighting goes beyond being physically fit to include being resilient to the stress and emotional effects of the job. For individual resilience, this means having the ability to prepare for and recover from stressful events so the responder can return to duty with some sense of normality. To accomplish this, responders must sleep well, eat right, and positively engage with peers.



Unmanaged, constant exposure to stress and adversity can affect relationships, cause health issues, hinder safety at work, and even lead to post-traumatic stress disorder ([PTSD](#)) and [suicide](#). Resilience begins with understanding the stressors that can lead to such negative consequences. Responding to the needs of a community during a crisis can have a lasting effect on the way emergency responders process the world around them. Being a resilient responder starts with a commitment to personal wellbeing by sleeping well, eating well, and living well.

Get a Good Night's Sleep

Resilience begins with reporting for duty [mentally and physically ready](#) to respond, which starts by being well rested. Getting adequate sleep is a critical component of one's physical health and mental wellbeing and is essential to resilience. Sleep helps the brain function and process the stressors of the world, according to the National Heart, Lung, and Blood Institute ([NHLBI](#)), which is part of the National Institutes of Health. Sleep also prepares the brain for duty by increasing attention span, decision-making abilities, and creative problem-solving skills.

NHLBI also points to the value of sleep in managing physical wellbeing and repairing the effects of stress on the body. When sleeping, the body heals and regenerates, and even has the ability to repair the heart and blood vessels affected by a variety of stressors. Alternatively, sleep deficiency can negatively affect emotions, behaviors, and ability to cope with changes. In turn, these emotional and behavioral changes can lead to elevated levels of stress, which have been linked to depression, risky behaviors, and even suicide. A continued lack of sleep can lead to other complications such as increased risk of heart disease, kidney disease, high blood pressure, diabetes, and stroke.

Take Time to Eat Right

To be resilient, responders also need to eat a healthy, well-balanced diet and avoid excessive amounts of caffeine and alcohol, which can interfere with sleep cycles and exaggerate stressors on the body and mind. Excessive amounts of alcohol or caffeine can also increase blood pressure, according to the [American Heart Association](#). Instead, firefighters need to drink large amounts of water to stay hydrated.

Although stress initially may reduce appetite, stress eating can also become a significant problem, according to an article in [Harvard Health](#). Prolonged exposure to significant stress triggers the body's survival mechanisms, which includes an increase in appetite. If the body



perceives that stress is ever-present, it may cause a continuation of appetite. Stress eating can lead to overeating comfort foods that are high in fats and sugars, which in turn can cause weight gain and lead to obesity.

Stress can also change the type of food desired. Several studies, including one published in February 2012 by the "[Harvard Mental Health Letter](#)" have shown that "physical or emotional distress increases the intake of food high in fat, sugar, or both."

Foods that are heavy in fat and sugar may interfere with the area of the brain that identifies stress. These comfort foods may reduce stress but create cravings for what may be unhealthy choices. To counteract the cravings for unhealthy food choices, firefighters need to focus their food choices on fruits and vegetables and limit the intake of foods high in fat, salt, and sugar. In addition, drinking water and exercising have the ability to lower levels of the stress hormone cortisol.

Engage Peers, Partners & Friends

Having healthy relationships is a critical component of a personal resilience strategy. Being mentally prepared for duty includes having the ability to process and discuss experiences with trusted people. Strong relationships help responders maintain a positive and calm outlook. It is essential to have a [support structure](#) to be resilient and have the ability to recover from stressful events.

The American Psychological Association ([APA](#)) released an online brochure that can assist individuals in building resilience. Two factors that they associate with resilience are communication skills and the capacity to manage strong feelings and impulses. Although an individual can build these capabilities alone, having relationships allows peers, partners, and friends to be part of their support network. Also, being there for others in need can be beneficial to building personal resilience. Strong relationships with others create environments where changes in personalities and behaviors can be recognized and mitigated early.

No one is immune to the physical and emotional impacts of stress. Just as physical conditioning takes time, building a resilient lifestyle takes time. However, it is an essential component of ensuring fitness for duty.

A previous version of this article was originally published in "[In Public Safety](#)" on 16 May 2017. Reprinted with permission.

Anthony S. Mangeri, MPA, CPM, CEM, is on the faculty of the American Public University System. He has more than 30 years of experience in emergency management and public safety. He has been a volunteer Firefighter and Emergency Medical Technician for more than 30 years. He earned the rank of assistant chief-safety officer, serving as the fire department's health and safety officer for three years. During the terrorist attacks of 9/11, he served as operations chief at the New Jersey Emergency Operations Center, coordinating that state's response to the passenger-aircraft crashes into the World Trade Center. He earned a Master of Public Administration from Rutgers University and is a Certified Public Manager. He has been awarded the designation of Certified Emergency Manager. He also sits on the ASIS Fire & Life Safety Council. In addition, he has completed a Fellowship in Public Health Leadership Initiative for Emergency Response sponsored by the Center for Public Health Preparedness.

EMERGENCY SERVICES WEBINAR SERIES 2017

KNOWLEDGE WHEN YOU NEED TO RESPOND

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

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

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

REGISTER FOR THE WEBINAR SERIES TODAY AT
[PUBLICSAFETYATAMU.COM/ DPJ](http://PUBLICSAFETYATAMU.COM/DPJ)

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

