



Highlights:

[Fire/EMS Response to Mass Violence Incidents](#)

[Wildfire Response Aided by Drone Aircraft](#)

[Insider Threat Awareness Virtual Roundtable](#)

[The Great SouthEast ShakeOut Set for October](#)

Disclaimer of Endorsement:

The EMR-ISAC does not endorse the organizations sponsoring linked websites, and does not endorse the views they express or the products/services they offer.



The U.S. Fire Administration maintains the **Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC)**.

For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: (301) 447-1325 and/or emr-isac@fema.dhs.gov.

The InfoGram

Volume 12 – Issue 33

August 16, 2012

Fire/EMS Response to Mass Violence Incidents

Several high-profile mass shootings made national headlines recently, each with unique circumstances. “[Response Priorities for Mass Violence Incidents](#)” in the June 2012 issue of Fire Engineering gives guidance for fire and EMS agencies on how to deal with and plan for active shooter incidents. Things to consider:

- Recognize that law enforcement will take the lead during the tactical stage until the scene is secured, and act accordingly.
- Assume details from dispatch may not be correct or complete, especially if it is based on public eye-witness accounts of a rapidly-changing situation.
- Identify the location of the command post and staging areas and coordinate fire and EMS response with other agencies on site.
- Understand response may happen in waves (e.g., SWAT as the first wave tracking the suspect, EMS as the second wave treating wounded, etc.).

Mass violence or active shooter incidents can and do happen in all types of urban and rural areas. As always, proper planning, drills, and coordination with local agencies and neighboring jurisdictions is key to successful response.

(Source: FireEngineering.com)

Wildfire Response Aided by Drone Aircraft

Unmanned Aerial Vehicles (UAVs), also known as “drone” aircraft, are being used in wildland fire response more now since the Federal Aviation Administration (FAA) authorized government agencies and private entities to operate unmanned aircraft in domestic airspace.

Armed with infrared heat-sensing equipment, the aircraft can detect not only the location of the active fire perimeter but also where hotspots may ignite new fires. The “drones” also act as communications hubs, transferring data like a network between areas.

[CNN reports](#) this technology has been around for a while, but until recently the thermal detectors could only get good data during night flights. This created a time lag between the data collection and creation of usable maps. Sometimes several hours would have passed, during which time the fire could have moved, changed direction, etc., by the time work starts during daylight hours.

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.

While the UAVs use is rare at the moment, their use is expected to rise when the technology becomes more accessible and cost-effectiveness is proven. Collected data will probably be helpful to scientists studying the movements of wildland fires as well as those studying the aftereffects.

(Source: [CNN](#))

Insider Threat Awareness Virtual Roundtable

The Department of Homeland Security's Office of Infrastructure Protection will be hosting a live 1-hour "[Insider Threat Awareness Virtual Roundtable](#)" on Tuesday, September 18, 2012, from 2-3 p.m. EDT.

Insider threat to critical infrastructures is when one or more persons with intimate knowledge of a company or organization use that knowledge to exploit known vulnerabilities with the intent to cause harm.

Subject matters experts will discuss three types of insider threats: physical/cyber sabotage, theft of intellectual property, and fraud. How malicious insiders impact organizations, how to deter and detect such threats, and what strategies are available to mitigate the threats will be covered.

Interested parties must [register to participate before September 14, 2012](#). Address any questions to stopinsiderthreat@hq.dhs.gov. A limited number of phone lines will be available to participants. If possible, please plan to listen using your computer's speakers.

(Source: [DHS](#))

The Great SouthEast ShakeOut Set for October

2012 is the fourth year for the [Great ShakeOut program started in California](#), and this year will be the first for the Southeastern United States and will include Georgia, North and South Carolina, Virginia, Maryland, and the District of Columbia. The voluntary [Great SouthEast ShakeOut](#) drill will be held October 18 for businesses, families, schools, and government agencies to learn and practice what to do when an earthquake occurs.

While there isn't much attention given to major earthquakes in the southeast United States, there have been a few of note. South Carolina was hit with a [7.3 magnitude quake](#) in the late 1800s, and [Virginia had a 5.8 magnitude quake](#) a year ago. Earthquake preparedness in this region of the country isn't given as much attention as hurricanes, for example, which makes public education on preparedness measures so essential.

[Resource materials](#) available include manuals for businesses, schools, non-profit organizations, and government agencies and facilities. There are also many ready-made flyers for more specific fields such as preschools, museums, healthcare facilities, organizations for seniors, etc. There is also a guide for people with disabilities and special access needs.

Interested parties can [register for the Great SouthEast ShakeOut](#) to receive emails, information, and tips on how to prepare. There are also other ShakeOut exercises being planned [across the country and overseas](#).

(Source: [Great SouthEast ShakeOut](#))

Fair Use Notice:

This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law.

If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local [FBI office](#) and also the [State or Major Urban Area Fusion Center](#).

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at 202-282-9201, or by email at nicc@dhs.gov.