EMR-ISAC
Emergency Management & Response-Information Sharing & Analysis Center

Highlights:

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 14 – Issue 9 *February 27, 2014*

Yarnell Hill Wildfire Talking Point Resources

The Wildland Fire Lessons Learned Center (LLC) gathered a collection of official documents on the Yarnell Hill Wildfire in Arizona, which killed 19 members of a hotshot crew due to entrapment. The Wildland Fire LLC suggests using the posted information during the annual fireline safety refresher training.

The collection consists of several investigation reports, maps, photos, a memorial book with information about the 19 members of the Granite Mountain Interagency Hotshot Crew that died, and a press kit. Also included is a PowerPoint presentation documenting how quickly the fire spread, pictures of the pre-fire fuels, and topographical maps.
The 23-minute narrated Serious Accident Investigation Briefing video uses 3-D mapping to show a timeline of events, communications, and leadership decisions in relation to the crew's location and fire spread leading up to the accident. The video shows in detail the circumstances of the incident, including the weather system that caused the shifted winds and the questions regarding the crew's intentions.

Many things are unknown surrounding this entrapment; however, the information provided about this tragedy provides talking points on a sensitive subject, helping crews learn from the incident.

(Source: Wildland Fire LLC)

9-1-1 Texting to be Implemented by Year End

This month, the Federal Communications Commission (FCC) proposed major wireless carriers be able to deliver text-to-9-1-1 by the end of 2014. The four major wireless providers already committed to making the feature available by May 2014 (PDF, 103 Kb) in areas where PSAPs have the technology in place to handle the service. The FCC applauded this move, but says more needs to be done to make the service more evenly available.

The updated proposal notes the public's increasing use of texting. The actual regularity that people are currently sending texts to 9-1-1 centers is unknown, nor is the number received known. However, Emergency Management magazine stated over 30,000 text-to-9-1-1 messages to a PSAP in Virginia went unanswered in 2013 due to the center's inability to receive them.

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

Due to this very possibility, the FCC adopted a "bounce-back" rule in areas where text-to-9-1-1 is not available. If a person sends a text to a 9-1-1 center where the service does not yet exist, the person will receive an automatic message declaring the message has not reached 9-1-1.

As PSAPs move forward with next generation 9-1-1, debates continue as to its efficacy during emergencies. Texting is now a primary means of communication for the 40+ million Americans with hearing or speech disabilities; however, the FCC maintains voice-based 9-1-1 is still the preferred method.

(Source: FCC)

Improving Critical Infrastructure Cybersecurity

The new 41-page guide "Framework for Improving Critical Infrastructure Cybersecurity" (PDF, 473 Kb), described as a "how-to" guidebook for owners and operators of critical infrastructure facilities, helps begin the process of shoring up cyber risks. The guide was developed by the National Institute of Standards and Technology (NIST) in response to the Presidential Order requesting it a year ago.

The guide's summary states the document was developed in such a way as to develop cybersecurity methods and actionable strategies without imposing more regulation on business and industry. The voluntary framework is designed to complement existing cybersecurity processes and programs, not replace them.

Cybersecurity is an increasing threat, and as critical infrastructure industries become more computer-based, automated and networked, the threat of disruption or destruction grows. That threat is quickly transferred to other industries thanks to the interconnection between sectors. Ensuring cybersecurity measures are in place for one helps secure all others from cascading failures.

(Source: NIST)

What Proactive Preparedness Looks Like

Years before the devastating flooding in Boulder, Colorado last September, emergency managers and city officials had been planning for such an event. Officials knew the serious risk of flooding in their area due to a variety of factors:

- Location – at the foot of the Rocky Mountains, heavy rains would funnel runoff directly towards the populated area;
- History – floods in 1969 and 1979 both served as testimony to the vulnerability of Boulder to flooding;
- Wildfire scars – the Fourmile Fire near Boulder in 2010 increased flash flood risk due to the lack of vegetation in the burned out areas;

Emergency managers in the Boulder area staffed their Emergency Operations Center when the "worst-case scenario" forecast came out, not waiting for the rains. Communications, pre-planned messaging, supply chain logistics, and interagency collaboration were all in place.

While there are still areas for improvement, the long-range planning of agencies in the Boulder area is a model best practices illustration to be studied and replicated.

(Source: Emergency Management Magazine)

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**.