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

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 16 – Issue 34   *August 25, 2016*

NIOSH Flooding Resources for First Responder

While some parts of the country are plagued by drought, other areas are experiencing extreme storms and floods. During storm and flood response, responder safety is extremely important. Storm and flood cleanup activities can be hazardous; workers and volunteers involved with flood cleanup should be aware of the potential dangers involved, and the proper safety precautions they can take.

It is important to prepare in advance for anticipated response activities. Even in the event of last-minute emergency response, both employers and workers should be aware of the hazards and precautionary actions to prevent work-related injuries and illnesses in the field once rescue, recovery, and clean-up begin.

The National Institute for Occupational Safety and Health (NIOSH) storm and flood resources for emergency response provides guidelines and recommendations for different types of emergency responders. Firefighters, for example, should be aware of operating procedures, what to do if there are shortages in communication, firefighting, personal protective equipment, or debris dispersal.

EMS personnel also face hazards responding to disasters when lifting patients, equipment and participating in the emergency transport of patients in ground and air vehicles. Law enforcement often play a major role during an emergency response and should be aware of the above guidelines and recommendations, too.

Emergency response is hard work and it can be useful to assume there might be stress and fatigue involved with it, for all workers. Learn to manage worker fatigue and stress during operations. No matter your job, employee or volunteer, the public depending on your help is also dependent on your health and safety.

(Source: NIOSH)

3D Technology Causes Problems at Airport

The Transportation Safety Administration (TSA) regularly finds weapons in carry-on bags at airports, but recently one find stood out. Someone was trying to carry a handgun printed using a 3D printer onto a plane at the Reno/Tahoe, Nevada, Airport. It was a replica but was loaded with live ammunition.

When first made publicly available several years ago, one thing that caught the eye of law enforcement and security agencies was the possibility of printing weapons

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

that did not trigger metal detectors. This becomes more of a worry as the price of the printing technology drops. The threat doesn't end with firearms, almost anything can be printed including knives, handcuff keys, and Unmanned Aerial Systems (aka "drones"). Plans for such items are available online.

In reality, someone can get a gun a lot cheaper than they can a 3D printer and as we've seen, if someone wants one is not difficult even if there are good reasons why they shouldn't have one. The concern with this is the possibility of concealment from security screening. At this point the laws have not quite caught up with technology. The case at the Reno/Tahoe Airport shows again how important it is to maintain good situational awareness and never assume.

(Source: ATF)

Insider Threat More a Problem Than You Think

A recent study on data security shows insider threats are more of a concern than we thought. Respondents said "insider negligence is more than twice as likely to cause the compromise of insider accounts as any other culprit, including external attackers, malicious employees, or contractors."

One of the issues leading to such negligence is the amount and type of data workers have access to. Sixty-two percent of respondents have access to sensitive or confidential data when they don't need it for their jobs, and only a quarter of the companies monitor email and file activity, and those not too actively.

The Emergency Services Sector has seen an increase in ransomware attacks in the past few years and cybersecurity in general continues to be a concern, especially among medical and law enforcement agencies. While departments and agencies should prepare for ransomware attacks from outside, they also should look at how much sensitive information is readily available to employees and consider limiting access.

(Source: FBI)

National Preparedness Month and Media Toolkit

September is National Preparedness Month and this year the focus is again on communication. Ready.gov hosts a variety of resources to help people prepare for disasters, especially youth, older adults, and people with disabilities and other functional needs.

For agencies working to promote resiliency in their communities, there are a number of new resources available to help, and the focus is on social media. There are pre-written messages you can share on your social media channels as well as graphics, logos, and videos. This year, they also have pre-set hashtags to use, and suggest using emojis.

Each week has a theme to promote preparedness activities with the "Kickoff to National Preparedness Month" starting next week. Many of these resources will be available throughout the year as part of Ready.gov's collection of resources. Be sure to keep them in mind when planning outreach campaigns.

(Source: Ready.gov)