Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 17 — Issue 35 | August 31, 2017

Emergency Responder Health Monitoring and Surveillance Program

First responders and other emergency workers face serious health and safety hazards when working disasters and emergency incidents, and their employers should take steps to monitor their health and safety. Unfortunately, this is not always done.

The National Institute for Occupational Safety and Health (NIOSH) provides tools for health and safety monitoring through the U.S. National Response Team (NRT) Emergency Responder Health Monitoring and Surveillance (ERHMS) system, which includes guidelines for protecting emergency responders involved in various emergencies and settings, training, manuals, software, studies and other supporting information.

The ERHMS System Training course provides necessary tools for implementing health monitoring and surveillance of emergency response workers and outlines important procedures during pre-deployment, deployment, and post-deployment activities, including credentialing, risk communication and after-action assessments.

The ERHMS System - Leadership Training course introduces the ERHMS system to those responsible for planning and executing incident response activities. The intended audience includes local, regional, state, tribal and federal personnel who are responsible for the occupational safety and health of first responders and others who work disaster cleanup and recovery.

Both courses are free online and provide Continuing Education Units (CEUs). Anyone involved with the deployment and protection of emergency workers is encouraged to take the courses and also to review the other ERHMS resources available on the NIOSH website.

(Source: NIOSH)

FBI: preliminary 2016 law enforcement deaths statistics released

Preliminary numbers released by the FBI report 66 law enforcement officers killed in the line of duty in 2016. This is a shocking increase of 61 percent from 2015, which saw 41 officer deaths. A few other numbers:

- 17 officers were ambushed.
- Offenders used firearms in 62 of the 66 incidents.
- 50 officers were confirmed to be wearing body armor at the time.
- An additional 52 officers were killed in line-of-duty accidents.

See the FBI's press release for more numbers; final statistics will be available this fall.

(Source: FBI)

"Utah Model" for cybercrime response and resilience

When the Bureau of Justice Assistance (BJA) conducted a case study to find out

Highlights

U.S. Fire Administration

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

what a successful cybercrime program looked like, it chose the Utah Department of Public Safety (DPS) program as the model. Over the past 4 years, Utah DPS created a robust system collectively called the Utah State Cyber Intelligence Network to investigate, analyze and study cybercrime and the consequences of cyberattack to emergency management and critical infrastructures.

The "Utah Model" case study describes how Utah decided to take a proactive role addressing cybercrime after several successful cyberattacks against the state. Between 2009 and 2012, the state saw successful denial-of-service attacks, the theft of $2.5 million and hacks of personal health information. Utah estimates 30,000 attempted attacks per day in 2010; that number skyrocketed to 100-200 million in one day in 2016, a frightening increase.

The BJA presents this case study as a guide for other states and even local governments to gauge their own program and improve upon it. It details the process of creating the state's program and the stumbling blocks they faced, staffing and duties, cybercrime and evidence collection, working with legislatures to change criminal code, training and education, partnering with other agencies and much more.

(Source: Utah DPS)

Webinar: Preparing for Catastrophic Events

During a catastrophic event, the supply of resources and service delivery capabilities are often disrupted or are insufficient to support the needs of fire and emergency services operations. This is currently being seen in Texas as recovery efforts continue after Hurricane Harvey and the needs of the response outweigh available resources.

On Thursday, September 21, 2017 from 1:30 p.m. to 2:30 p.m. Eastern, the U.S. Fire Administration (USFA) is hosting the webinar "Preparing for a National Catastrophic Event." The USFA webinar will:

- Define what is considered a catastrophic event.
- Explain why it's necessary to prepare for catastrophic events.
- Outline three easy steps to assess your capabilities.
- Discuss actions local agencies can take that enhance national response.

The webinar will also introduce USFA's plans to conduct a formal survey of available and deployable fire service resources. This database would be used only during a catastrophic event when other resources are not available.

Those interested must register at the USFA website. Other upcoming webinars are listed, as are recordings of past webinars. All USFA webinars are free.

(Source: USFA)

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.**

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.