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

The InfoGram

Volume 18 — Issue 11 | March 15, 2018

TRANSCAER Crude by Rail Safety Course now available

The American Petroleum Institute (API) and Association of American Railroads (AAR) have finalized the Crude by Rail Safety Course. This course helps prepare first responders for incidents related to trains carrying crude oil.

The Crude by Rail Safety Course describes the characteristics of crude oil and the rail cars it is shipped in, the response strategies to be considered, firefighting and spill response considerations, and the need for structured incident management.

This course is meant to complement existing training and provide an accessible, easily distributed program to assist communities prepare for and respond to a possible hazardous materials transportation incident involving crude oil.

In addition to the safety course video, the DVD Extra's folder also includes the 2017 Field Guide for Tank Cars, AAR Pamphlet 34, U.S. DOT Chart 16, and links to other helpful crude by rail educational references.

The program is part of the TRANSCAER© National Training Tour. To request copies of the Crude by Rail Safety Course DVD or an in-person presentation, please send requests to cbrrequest@api.org.

(Source: TRANSCAER)

Exploring sUAS use in your fire and rescue department

Fire departments continue to evaluate using small unmanned aerial systems (sUAS) in their operations. Some departments have already created robust sUAS programs for a variety of potential uses, including:

- Scene size-up, pre-incident planning and damage assessments (PDF, 1.9 MB).
- Digitally mapping hazards, both urban and rural/wildfire areas.
- Search and rescue in remote areas.
- Hazmat scene/release evaluation.
- Deployment of automatic external defibrillators or other medical equipment.
- Video recording training, drills and exercises for later evaluation.

As an example, the Orange County (Florida) Fire Rescue Department now has seven pilots licensed to operate 10 sUAS and Federal Aviation Administration (FAA) certification. sUAS operations are not limited to large career departments with bigger budgets, though. A Missouri volunteer department recently gained national attention for their aerial video evaluating the scope of a recent 50-car pile-up.

With so many sUAS possibilities for the fire service, the National Fire Protection Association (NFPA) proposed a standard addressing minimum requirements for the operation, deployment and implementation of sUAS. Those interested can review the NFPA 2400 the document scope and sign up for email updates

When you look at everything a sUAS makes possible, the lure to get one is strong. Fire departments should complete a thorough needs assessment before investing

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.

time and money in equipment, training and getting an FAA waiver or authorization. Determining how you will use the sUAS will often determine what to purchase and who to train, ensuring money well spent instead of wasted.

(Source: NFPA)

Mistakes leaders make after a data breach

You just find out that your department or office had a serious breach and personal data was stolen. What do you do? More importantly, what don't you do?

Harvard Business Review took a look at mistakes commonly made by leaders faced with a data breach. While it does focus on business and corporate issues, much of the information translates to emergency service sector agencies and departments.

- **Waiting to notify victims**. The longer you wait to let those affected know, the longer criminals will be able to use the stolen data, and the more damage control you will be forced to handle, including your organization's reputation.
- **Assuming it won't happen**. A current buzz phrase is "cyber security is the new cold war." Whether it's a data breach or some other form of cyberattack, assume you will have to manage one sooner rather than later.
- **Not having a plan in place**. Having an incident plan goes a long way to instilling confidence in the organization to be able to handle a breach. Contact municipalities or organizations who've been affected to talk best practices.
- **Lack of transparency**. There is a difference between damage control and withholding vital information. Transparency promotes trust.

(Source: Harvard Business Review)

NIST updates Cybersecurity Framework website

Last month, the National Institutes of Standards and Technology (NIST) launched a major update to the Cybersecurity Framework website.

The Framework's prioritized, flexible and cost-effective approach promotes protection and resilience of critical infrastructure and other sectors important to the economy and national security. Updated features include:

- Background information for those who are new to the Cybersecurity Framework.
- Upcoming events and presentations.
- Resources and frequently asked questions to help organizations use the Framework.
- Perspectives from Framework users and Framework in the news.

The Cybersecurity Framework is voluntary, consisting of standards, guidelines and best practices to manage cybersecurity-related risk. The NIST website provides information and support to help organizations with their cybersecurity goals.

(Source: NIST)

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.