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

The InfoGram

Volume 16 – Issue 7 *February 18, 2016*

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.**

AAR: Crude by Rail Training for First Responders

Production of crude oil from the Bakken region is currently down, but the concerns surrounding the transportation of highly volatile crude oil still remains. The Association of American Railroads (AAR) in cooperation with seven major railroad companies, is now offering "Crude by Rail Web-based Training."

The 4-hour long training targets first responders who have railroads passing through their jurisdictions. It covers planning and working with the railroads; basic tank recognition and design; properties of the different types of crude; tactics and incident management; and more.

The training is available at no charge to first responders; there is a small fee to all others. The program is self-directed and can be taken at the student's convenience, and provides a foundation of needed information and practices students can put to work if faced with a crude by rail incident.

(Source: AAR)

Cybersecurity Takes Forefront in New Action Plan

News broke in December of a successful 2013 hacking attack of a dam in New York, during which Iranians obtained the ability to control the floodgates. This is not the first nor the last time for a breach like this, but each such attack serves as a warning of what could happen should the wrong people gain access to the wrong system and decide to finally stop playing around.

In fact, two examples of the possibilities came in just the last few weeks. Last month, a virus was introduced into the Israeli Electrical Authority, forcing them to "paralyze" many of their computers to keep the virus from spreading. A few weeks before that the Ukraine suffered the first known power outage caused by highly destructive malware, leaving hundreds of thousands of homes without power, a hazardous problem in a Ukrainian winter.

Experts point to these events and remind us that the dated industrial control systems running many critical infrastructure in the United States are just as vulnerable to attack, something first responder agencies and departments should consider when creating emergency and response plans. For example, not only would fire and public health be responding to incidents caused by a large-scale power outage, they will be forced to navigate their duties without power as well.

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

This week the president released his final budget proposal, containing direction for the creation of a Cybersecurity National Action Plan. The proposed plan includes an investment of $19 million for actions that would add extra layers of security for personal online accounts, modernize government technology to minimize breaches, assistance in securing "Internet of Things" devices, and catching and prosecuting cyber criminals.

(Source: The White House)

Countering Violent Extremism Website for Teens

High school students are perfect targets for recruitment by violent extremists seeking support for their radical ideologies, foreign groups looking for fighters, or for those who wish to conduct acts of targeted violence within our borders, as this is often the prime time for rebellion and trying to be different while looking for a way to still "fit in." There are several notable cases of teens and college students attempting to join the Islamic State of Iraq and the Levant (ISIL) in the past few years. While it remains an unlikely event, it does happen.

Most extremist recruiting techniques today focus on technology many parents didn't have in their youth: the Internet, texting, cellphones, and peripheral apps and websites. ISIL has been extremely successful using these mediums to recruit fighters and maintain their momentum, but other groups use them, too.

The FBI launched a new website designed to raise awareness of violent extremism and help keep teens from being radicalized and recruited. The site's message – Don't Be a Puppet – is geared to educate impressionable adolescents on the many ways recruiters may try to contact them and have them join their cause – whatever that cause may be. The interactive site uses videos, activities, and other materials to teach about violent extremism and ultimately to free the puppet figure that is displayed throughout.

Parents and high schools must be vigilant and educate their students about what drives violent extremism and the potential consequences of embracing extremist beliefs. Another resource to help this goal is the FBI report "Preventing Violent Extremism in Schools" (PDF, 1.53 Mb), released in January.

(Source: FBI)

SAFETY Act Webinar

The SAFETY Act, which stands for "The Support Anti-terrorism by Fostering Effective Technologies Act," was first introduced in the Homeland Security Act of 2002 as a way to provide incentives and liability protection for individuals and companies interested in developing and deploying anti-terrorism technology.

The types of approved technology already in use include explosive detection, cybersecurity applications, incident management software, cargo screening services, video management software, remote sensing, and more. Each qualified technology carries the SAFETY Act seal which buyers can seek out when researching goods and services. The designation does expire and developers must submit renewal paperwork to keep the designation current.

The Department of Homeland Security (DHS) is hosting a webinar on Wednesday, February 24th from 1:30-2:30 p.m. Eastern to discuss how to effectively submit SAFETY Act renewal applications. Interested parties should register.

(Source: SAFETY Act)

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**.