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

Highlights:

LEEDIR Leverages Citizen Witnesses

Someone Reports a Cyber Crime. Now What?

E-Cigarettes, Poisonings, and Illegal Drug Use

National Model EMS Clinical Guidelines Released

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 46   November 13, 2014

LEEDIR Leverages Citizen Witnesses

In the aftermath of the Boston Marathon Bombing, pictures taken by eyewitnesses during the incident played a large role in the capture of the suspects. At that time, the public response to the call for help was literally overwhelming, as a key problem with soliciting media from the public is storage of the large amount of data.

The Large Emergency Event Digital Information Repository (LEEDIR) may be a solution to that problem. LEEDIR helps agencies request and collect media from the public and store it on LEEDIR's Cloud for follow-up during an investigation.

Interested agencies can register for LEEDIR on their website and receive updates and training. Pre-registration and training makes it easier to activate the system quickly. In addition, the public may download the LEEDIR app for their iPhones or Android devices, enabling them to send in photos or video using their social media accounts.

LEEDIR is free to law enforcement and relief agencies if they meet these criteria:

- Involve multiple jurisdictions or disciplines, and
- Cover at least 5 square miles or have at least 5,000 people in attendance.

While these criteria may initially seem quite limiting, keep in mind events like strings of arsons, wildfires, crime sprees, and riots fit LEEDIR's terms. Current information requests are viewable on their website as well, as is a short overview video.

(Source: LEEDIR)

Someone Reports a Cyber Crime. Now What?

We hear constantly that cybercrime is increasing. Data breaches in big business seem to make headlines weekly now, and nearly everyone knows the risks of malware on their computers and mobile devices. But say your department or agency is the victim of a cyber incident. Who do you call? What do you do if a citizen or local business calls you to report a cyber incident?

"Law Enforcement Cyber Incident Reporting" (PDF, 535 Kb) answers questions state, local, tribal, and territorial (SLTT) agencies may have about cybercrime reporting. Published by the Department of Homeland Security, the concise, 2-page information sheet provides answers, contact information, and training resources to help address cybercrime.

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

A cyber incident should be reported if it:

- May impact national or economic security or public health and safety;
- Affects core government or critical infrastructure functions;
- Results in a significant loss of data, system availability, or control of systems;
- Involves a large number of victims.

The sheet also details exactly what information is necessary to report and what would be nice to have. The guide lists the agencies to contact for specific types of cyber incidents. Finally, several training and resource links provide more support for SLTT agencies looking to strengthen their knowledge of and response to cybercrimes.

(Source: [U.S. Secret Service](#))

E-Cigarettes, Poisonings, and Illegal Drug Use

Primarily marketed as a tool to help people quit smoking, the e-cigarette is a battery-powered vaporizer billed as being safer than regular cigarettes. The vaporizer heats a liquid solution containing nicotine and other chemicals, creating a mist.

E-cigarettes are fairly easy to get and have much less stigma than cigarettes, and even have a growing popularity. Due to this, there is an increase in their use among teenagers. This is concerning because it can lead to lifelong nicotine addiction, and medical groups have raised concerns about the [lack of e-cigarettes regulation](#).

Unfortunately, there is also a [growing trend to use e-cigarettes as a way to "smoke" illegal drugs](#) such as marijuana, hash oil, or the synthetic drug spice. It is easier to hide and it doesn't smell as strongly as smoking marijuana does. Sites like YouTube have many videos available on adapting vaporizers for illegal drug use.

In addition, there are some reports of [children coming into contact with e-cigarette liquid nicotine refills accidentally](#), which can cause nicotine poisoning. The candy or fruit flavors draw them. Poisoning can occur by swallowing the liquid, inhaling the vapor, or absorbing the liquid through the skin. It can cause nausea, vomiting, and seizures.

EMS workers should be on the lookout for the symptoms of nicotine poisoning in children listed above. They should also be aware of the symptoms of the [illegal drug spice:](#) agitation, sweating, trouble breathing, racing pulses, confusion, and hallucinations.

(Source: [DrugAbuse.gov](#))

National Model EMS Clinical Guidelines Released

The National Association of State EMS Officials (NASEMSO) announced the completion of the "[National Model EMS Clinical Guidelines](#)." Intended to be a "comprehensive set of EMS performance measures," the guidelines can be adopted by state EMS systems as a whole or in parts. The guidelines are not intended to be mandatory.

The guidelines offer a more standardized approach by providing uniformity in patient care. They also serve as a standard on which EMS medical directors can base practice. NASEMSO plans on updating and adding to these guidelines over time.

This current document is consensus-based, and the long-term goal is to update it with evidence-based guidelines as they are developed. The 2-year project was undertaken in cooperation with the National Highway Traffic Safety Administration.

(Source: [NASEMSO](#))

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**.