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

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**.

The InfoGram

Volume 13 – Issue 41 *October 24, 2013*

Krokodil: Deadly Drug May Be in United States

The street drug Krokodil may have made its way to the United States from Russia, where it is a popular and less expensive alternative to heroin. News sources have reported unconfirmed cases in Arizona, Chicago, and New York in the past few weeks. The life expectancy of someone who is a regular Krokodil user is 2-3 years.

The drug desomorphine is an opiate first developed in the 1930s. According to the Drug Enforcement Agency (DEA)'s fact sheet on desomorphine (PDF, 56 Kb), there is no legal use for this drug today. This is another example of a drug that can be cheaply and relatively easily made in a home lab, and instructional materials are showing up on the internet.

Krokodil gets its name from its ability to eat away and rot a person from the inside by destroying blood vessels at injection sites, leaving the skin scaly and green. Users can die from gangrene, infection, and loss of skin. Amputations are common. The drug may be 3-10 times cheaper than heroin in the United States and Russia, and the DEA is concerned about its possible appearance here.

While the cases have not been confirmed, first responders should be aware of the possibility of this drug being in the United States and familiarize themselves with the signs, symptoms, and treatment.

(Source: NIH)

NIMS: Intelligence, Investigations, Field Ops

The National Incident Management System (NIMS) provides a reliable framework for government agencies, the private sector, and other organizations to respond cohesively to a range of different incidents. When the cause of an incident is not known (power failure, explosion, anything that has a possible nexus to terrorism), an investigation is required.

NIMS: Intelligence/Investigations Function Guidance and Field Operations Guide was released by the Federal Emergency Management Agency (FEMA) this month to provide guidance on how to integrate the Intelligence/Investigations Function into NIMS concepts and principles. The document shows how this function fits into the Unified Command or Incident Command System to possibly include forensic, intelligence, missing persons, mass fatality management, and investigative branches.

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

The fire service, medical community, and law enforcement are the three fields most affected by this function. Investigations are often carried out by law enforcement. However, the guide stresses common examples of investigations carried out by other entities to include epidemiology; transportation accidents; explosions, fires, or arson cases; research to support response or recovery efforts; and mass fatalities.

(Source: FEMA)

Cybersecurity for Public Safety Webinar

The First Responders Group Capacity Building Webinar Series, hosted by the U.S. Department of Homeland Security (DHS) Science and Technology Directorate, is holding the Cybersecurity Overview for Public Safety Administrators on Thursday, November 7 at 1 p.m. EST. There is no cost to participate in this event, which will last approximately 1 hour and 15 minutes.

The webinar series aims to foster innovation and learning to address evolving challenges of first responders and homeland security enterprise. The series highlights emerging technologies, research, best practices, and lessons learned to ensure the nation is safe, secure, and resilient against terrorism and other hazards. Recordings of past webinars are available at the webinar series' website.

Presenters for this webinar will include the chair of the Emergency Services Sector (ESS) Cyber working group and DHS officials from the ESS branch of the Office of Infrastructure Protection, the Cybersecurity Division of the Science and Technology Directorate, and the Industry Engagement and Resilience Branch of the Office of Cybersecurity and Communications.

(Source: DHS Science & Technology Directorate)

Equipment, Training for Active Shooter Events

Since the school shooting in Sandyhook, CT, and the shooting in Webster, NY, there has been a notable increase in information requests and interest in preparing for active shooter events. Texas State University's Advanced Law Enforcement Rapid Response Training (ALERRT) program published a study which looks at equipment and training requirements based on active shooting events from 2000-2010.

United States Active Shooter Events from 2000 to 2010: Training and Equipment Implications (PDF, 363.6 Kb) provides a concise statistical breakdown of 84 active shooter events including types of weapons used, how the events were resolved, number of people shot, and attack location. Based on this information, training and equipment needs were identified to include the following:

- Shooters go outdoors 20 percent of the time, so responders should be trained to manage and contain incidents outside;
- Attackers can and do use weaponry that will breach standard body armor, law enforcement must have adequate protective gear;
- Responders should be prepared to breach doors as some shooters try to slow responders down by barricading entrances;
- Incidents ended by force 28 percent of the time. Law enforcement must be willing and able to make the call to use deadly force if it becomes necessary.

(Source: ALERRT)

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**.