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

The InfoGram

Volume 16 – Issue 3 *January 21, 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.**

Webinar: Successful Body Worn Camera Programs

The International Public Safety Association (IPSA) is hosting a free webinar a on a hot topic to the law enforcement community. The "Implementing a Successful Body Worn Camera Program in a Post-Ferguson Era" webinar aims to assist departments in the decision of whether or not to utilize body-worn cameras. This webinar will be held Wednesday, January 27th from 2:00-3:00 pm EST. Registration is required.

The push for body-worn camera use by law enforcement increased after the shooting incident in Ferguson, MO. The theory is that they will provide accountability, increase community trust, reduce the number of complaints against law enforcement, and help with officer safety.

A representative from the Pasco County (Florida) Sheriff's Office will talk about its recent implementation of body-worn cameras agency wide and how it has been a positive move for them. This webinar will cover effective communications strategies, policy development, training, data storage, Freedom of Information Act (FOIA) requests, and more.

Departments interested in more information on body-worn cameras can take a look at the Bureau of Justice Assistance's National Body-Worn Camera Toolkit, a clearinghouse resource providing more information on policy, research, training, and technology.

(Source: IPSA)

Proposed Deductible for Disaster Declarations

Recently, the Government Accountability Office and the Department of Homeland Security recommended to the Federal Emergency Management Agency (FEMA) a need to raise the threshold for disaster declarations. FEMA believes raising the disaster declaration threshold would put too much of a burden on taxpayers and is proposing a disaster deductible instead.

FEMA is asking for state, local, tribal, and territorial emergency managers for comments on this proposed action. Currently the proposed rule would set a deductible and have incentives in the form of mitigation efforts and strategies which would effectively "buy down" future risk. FEMA believes that in addition to avoiding raising the disaster declaration threshold, the proposed deductible will motivate recipients to plan and enact mitigation efforts while also increasing stakeholder investment.

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

The full text of the proposed rule and instructions for comments are available on Regulations.gov. In addition, FEMA lists specific questions it would find particularly beneficial to have addressed. Comments on this proposed rule are due by March 21, 2016.

(Source: Regulations.gov)

The Role of EMS in Ending Human Trafficking

January is National Human Trafficking Awareness Month, and the Blue Campaign to End Human Trafficking requests the participation of EMS departments in a webinar next week on how they can help end this terrible crime.

The webinar will cover signs of human trafficking that EMS personnel should be trained to recognize, and what they should do if they should find potential victims. Presenters include the Department of Homeland Security's Assistant Secretary for Health Affairs and Chief Medical Officer. There will be a question and answer period. Those interested are asked to register.

The webinar is scheduled for Monday, January 25 at 2 p.m. EST. It is part of the EMS Focus webinar series, held every-other month. Previously aired webinars are available on their website for review.

(Source: EMS.gov)

Back to Basics: Information Security

The military term OpSec stands for Operations Security, the process of limiting an adversary's ability to gather critical information from various sources, compile it, and ultimately use it against us. An example of the OpSec fight in World War II was the "Loose Lips Sink Ships" campaign. One key OpSec measure, Information Security (InfoSec), guards against unapproved access, use, or altering of information, either paper information or electronic.

Both OpSec in general and InfoSec specifically are useful tools for the Emergency Services Sector due to the amount and types of information they regularly use. For example, departments in cities that could be targets of terrorist activity should guard against "advertising" Standard Operating Procedures, facility diagrams, personnel specifics, and exercise or training details online as terrorists could exploit their vulnerabilities. Departments in smaller communities should also do so, but more to guard against being the victim of criminal activity.

Much of InfoSec has veered into the realm of cyber security in the past couple decades. It goes beyond not writing down usernames and passwords and leaving them lying around. With the advent of hackers targeting first responder agencies, it is important to maintain effective barriers against hackers, viruses, worms, and to educate employees about phishing attacks and other social engineering tactics.

Finding a reasonable balance between good community relations and InfoSec is up to each individual department and will depend on a number of factors, including what legally must be disclosed under state law. However, good operational security will benefit every department.

(Source: FTC)

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**.