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

The InfoGram

Volume 18 — Issue 29 | July 19 , 2018

DOJ launches Violence Reduction Response Center

Last month, the U.S. Department of Justice (DOJ) launched the Violence Reduction Response Center (VRRC), a new "one-stop shop" to help connect state, local and tribal justice agencies, and the public, with violent crime reduction resources, training and technical assistance.

VRRC staff can direct callers to available grant-funding opportunities, training programs and subject-matter experts on violence reduction strategies. VRRC's goal is to reduce the time a caller spends seeking out this information themselves.

Agencies can contact the VRCC for assistance Monday through Friday between 9:00 a.m. to 5:00 p.m. Eastern via their toll-free number 1-833-872-5174, or anytime via email at ViolenceReduction@usdoj.gov. Calls or emails received after business hours will be returned within one business day.

The VRRC comes to fruition approximately 7.5 months after it was first announced as part of an overall plan to reduce violent crime in the United States. It falls under the Bureau of Justice Assistance National Training and Technical Assistance Center.

(Source: DOJ VRRC)

Countering false social media information

The internet has been a hotbed of false and inaccurate information since its beginning. Countering it remains a constant problem for any organization, company, department or agency trying to help the public stay healthy, safe and informed.

The Department of Homeland Security's Social Media Working Group for Emergency Services and Disaster Management provides recommendations to the emergency preparedness and response community on the use of social media technologies. They recently published the white paper "Countering False Information on Social Media in Disasters and Emergencies" to help agencies with this issue.

The white paper examines what motivates people to share bad or false information and discusses underlying issues that cause false information. It looks at several real-world case studies to provide agencies several best practices to counter misinformation, rumors and false information.

False social media content is most often caused by four issues:

- Incorrect Information (intentional versus unintentional).
- Insufficient Information.
- Opportunistic Disinformation.
- Outdated Information.

The white paper examines each of these issues in depth with examples. Further, key best practices are explored and categorized by people, processes, and technology. These include partnerships, software considerations and advanced preparation. Additional considerations and challenges that may be encountered are also included for reference.

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.

Members of the working group are subject-matter experts from federal, tribal, territorial, state, and local responders. They establish and collect best practices and solutions to be implemented by public safety officials and first responders.

(Source: DHS)

Starting a law enforcement agency-based cybercrime unit

Work on cyber-related crime is new territory for many law enforcement agencies and, as such, finding reliable resources to assist departments through investigations can be challenging. Fortunately, more resources are coming available to fill this gap.

The Law Enforcement Cyber Center (LECC) supports agencies investigating and preventing crimes involving electronic devices and components, to include digital forensics and information security. It is a collaborative project between several national organizations and is funded through the Bureau of Justice Affairs.

The LECC provides links to training, updated information on cyber threats, investigative resources, a directory of cybercrime labs and instructions on incident reporting. These resource make cyber topics easily accessible, even for someone new to the topic.

For those departments considering developing a specialty team, the Police Executive Research Forum offers "Starting a CyberCrime Unit: Key Considerations for Police Chiefs" (PDF, 491 KB). This document concisely covers needs assessment and scope, training and staffing needs, interagency partnerships, and funding and budgetary issues to address.

The report provides examples of things to consider in each step and suggestions of places to find free or inexpensive training. This report is a good initial step in deciding if a cybercrime unit is the right move for your department.

(Source: LECC)

Webinar: Office for Bombing Prevention programs for first responders

On Thursday, July 26, 2018, from 1-2 p.m. Eastern, the Department of Homeland Security's Office for Bombing Prevention (OBP) is hosting a webinar to discuss OBP programs and information sharing efforts supporting first responders. Those interested must register.

Specifically, the webinar will discuss several Counter-Improvised Explosive Device (C-IED) information sharing programs such as the Technical Resource for Incident Prevention (TRIPwire) site, a variety of training programs, C-IED Capability Assessment and Planning, Multi-Jurisdiction IED Security Planning, and the National Counter-IED Capabilities Analysis Database (NCCAD).

The mission of the OBP is to protect life and critical infrastructure by building capabilities within the general public and across the public and private sectors in order to prevent, protect against, respond to, and mitigate bombing incidents.

(Source: DHS OBP)

Fair Use Notice:
This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law.

If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

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.

Disclaimer of Endorsement: The EMR-ISAC does not endorse the organizations sponsoring linked websites, and does not endorse the views they express or the products/services they offer.