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

The InfoGram

Volume 20 — Issue 6 | February 6, 2020

PHMSA grants tackle safety awareness, training for first responders

The United States Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA) today announced it will accept applications for up to $12.5 million in grants for safety awareness, training, research and other activities to help communities avert or respond to hazardous materials-related transportation incidents.

Each year, PHMSA offers grants to state, tribal, non-profit and community-based organizations through its safety programs for the nation's pipeline network and hazardous materials transportation system. Grant recipients use the funds to train first responders, educate the public on local safety initiatives, develop and commercialize new technologies or participate in regulatory oversight activities.

The number of grant recipients receiving awards depends on the grant program, as well as the quality and number of applications received, the dollar amounts requested, and funding availability. Grant recipients are required to provide a report to PHMSA within one year chronicling completion of the work, as outlined in their grant agreement.

To obtain full eligibility requirements and application instructions, please search "PHMSA" on Grants.gov. Applicants can also contact the appropriate agency representative within the notice of funding opportunity announcement of interest.

(Source: PHMSA)

Coronavirus updates, interactive map, guidance now available

Though the vast majority of 2019 Novel Coronavirus (2019-nCoV) cases are still in China, the virus continues to spread around the world. The Centers for Disease Control and Prevention (CDC) reports 11 confirmed cases in the United States, 206 negative results, 76 results pending and zero deaths, as of February 5, 2020.

According to the interactive worldwide map maintained by Johns Hopkins University, as of this writing there were 28,344 confirmed cases and 565 deaths. The World Health Organization (WHO) reports slightly lower numbers.

The Los Angeles County of Public Health produced a two-page Frequently Asked Questions for first responders on 2019-nCoV (PDF, 172 KB). It covers how the virus is spread, typical symptoms and how first responders can protect themselves.

First responders should monitor the CDC and WHO site and stay in touch with their state and local public health departments to stay up-to-date on developments that may affect them and their region.

(Source: CDC)

DEA releases annual findings on country's drug threat

Last month, 11 correctional facility mailroom employees went to the hospital after an accidental fentanyl exposure. One corrections officer had to be treated with Narcan and the mailroom needed to be decontaminated before being put back in to service. The incident prompted New York state lawmakers to call fentanyl a public health crisis.

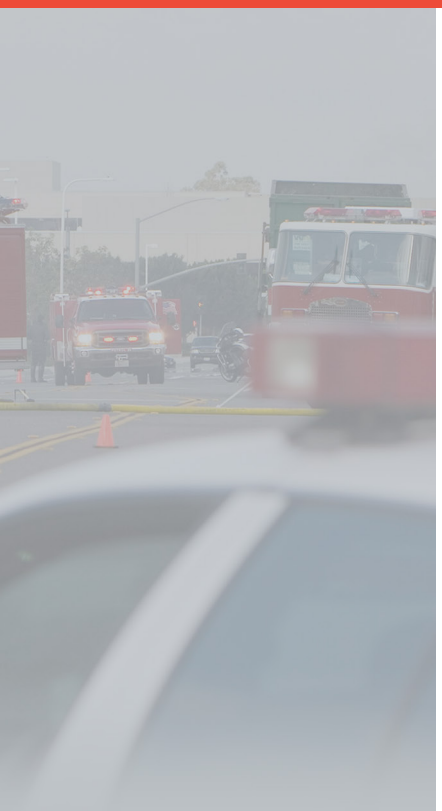
Highlights

U.S. Fire Administration

The U.S. Fire Administration operates 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.

Subscribe here



The changing drug environment affects first responders through increased EMS calls, fluctuating crime rates, threats to public health and other associated concerns. In turn, agencies must keep up with the changing threat environment in their regions, ensuring personnel is well-prepared in an effort to save lives.

In its 2019 National Drug Threat Assessment (PDF 8.3 MB), the Drug Enforcement Agency (DEA) calls fentanyl the most lethal category of illicit substances misused in the United States. It is only one of many substances highlighted in the annual report that first responders should be both aware of and ready for during their duties. Other highlights from the 2019 report:

- Cocaine is seeing a comeback. Cocaine-related overdose deaths are higher than expected due to fentanyl in the cocaine supply.
- Marijuana is still the most commonly used illicit drug. As states legalize marijuana use, most have not put limits on the potency and as the levels of tetrahydrocannabinol (THC) increase, so does demand.
- Controlled prescription drugs account for the most drug-involved overdose deaths in the country and are the second most abused substances.
- New for the 2019 report is a section on gang activity.

(Source: DEA)

Security and Resiliency Guides help you prepare for IEDs

Law enforcement and security managers interested in enhancing their posture against potential improvised explosive devices (IEDs) should check out the Security and Resiliency Guides (SRG C-IED) produced jointly by the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI.

The guides and guide annexes are designed to help stakeholders take proactive steps against IEDs by providing guidance and resources consistent with broader all-hazards preparedness and risk management principles. The guide integrates the contributions of numerous counter-IED (C-IED) subject matter experts, stakeholders, and professional communities.

The annexes for Lodging, Outdoor Events, Public Assembly and Sports Leagues/Venues provide security managers and staff with tailored information to improve preparedness. Through these annexes you can:

- Gain a better understanding of existing C-IED practices and needs.
- Obtain information to support preparedness efforts, such as risk assessments, planning, equipment purchases and staff training.
- Collaborate and communicate more effectively with venue counterparts, community first responders and government agencies.

The guide can help start or continue a conversation about bombing prevention between leadership, security managers and staff, empowering all members of an organization to play a role in security.

If you would like to engage the OBP team in discussion about how you and your team can increase your preparedness to prevent, mitigate and respond to bombing incidents, please reach out to us at OBP@cisa.dhs.gov or contact CIOCC.physical@cisa.dhs.gov to be connected with your local Protective Security Advisor (PSA).

(Source: CISA)

Cyber Threats

Coronavirus exploited to deliver malware, phishing, hoaxes

The Wuhan coronavirus continues to spread and create anxiety across the globe, allowing malicious individuals and groups to **exploit the situation to spread fake news, malware and phishing emails**.

IBM X-Force says that Japanese users have been receiving fake notifications about the coronavirus spreading in several prefectures, purportedly sent by a disability welfare service provider and a public health center.

The emails contains legitimate information taken from those services' official websites and carries an attached .doc file that ostensibly contains more information.

(Source: HelpNetSecurity)

Hackers are hijacking smart building access systems

Hackers are actively searching the internet and hijacking smart door/building access control systems, which they are using to launch DDoS attacks, according to a firewall company.

Linear eMerge E3 devices fall in the hardware category of "access control systems." They are installed in corporate headquarters, factories or industrial parks. Their primary purpose is to control what doors and rooms employees and visitors can access based on their credentials (access codes) or smart cards.

(Source: zdnet)

New York wants to ban paying ransomware demands

While it is advised that ransomware victims never pay their attackers, many businesses and even governments still do, which is why two state senators from New York have proposed bills banning local municipalities and governments from using taxpayer money to pay ransomware demands.

The bills introduced by the New York Senators represent **the first time state authorities have proposed a law that explicitly forbids local municipalities and governments from paying a ransom following a ransomware attack**.

(Source: MSN.com)

NSA releases information sheet on mitigating cloud vulnerabilities

The National Security Agency (NSA) has released an **information sheet with guidance on mitigating cloud vulnerabilities**. NSA identifies cloud security components and discusses threat actors, cloud vulnerabilities, and potential mitigation measures.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages administrators and users to review NSA's guidance on Mitigating Cloud Vulnerabilities and CISA's page on APTs Targeting IT Service Provider Customers and Analysis Report on Microsoft Office 365 and other Cloud Security Observations for information on implementing a defense-in-depth strategy to protect infrastructure assets.

(Source: CISA)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

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