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

The InfoGram

Volume 20 — Issue 37 | September 10, 2020

COVID-19 responsible for most line of duty deaths so far in 2020

Both the Officer Down Memorial Page and the National Law Enforcement Officers Memorial Fund have recorded more COVID-19-related deaths than those attributed to gun violence, vehicle-related incidents and all other causes combined so far in 2020. Both list about 100 law enforcement deaths from COVID-19. Fire and EMS deaths related to the coronavirus are also up according to several sources.

The law enforcement cases reported above are confirmed to have been work-related, and Officer Down is verifiying another 150 deaths at this time. There is a chance COVID-19 may double overall line of duty deaths among both the fire service/EMS and law enforcement before this is done.

According to a survey of first responders, firefighters are the group least likely to wear masks in buildings despite substantial evidence showing their efficacy. It is extremely important all first responders take the necessary recommended precautions to reduce exposures and help prevent the spread of the coronavirus.

EMS.gov, the U.S. Fire Administration and the Centers for Disease Control and Prevention all list recommendations to help first responders more safely do their jobs.

COVID-19-related first responder deaths are considered line of duty deaths. Legislation passed in August provides first responders who die from or are disabled by complications related to COVID-19 a statutory presumption that they contracted the virus on the job. Prior to this, suspected cases were required to have proof that exposure occurred during the course of their work duties.

(Sources: Various)

NACCHO releases 2019 National Profile of Local Health Departments

The National Association of County and City Health Officials (NACCHO) recently released the 2019 National Profile of Local Health Departments. It is an all-inclusive survey of local health department (LHD) funding, workforce programs and partnerships. It also looks at how things have changed over time.

One of the key benefits of this research is to compare how services and capabilities have changed since the last survey 3 years ago. NACCHO found three key items:

- **Workforce capacity is down**. Local health departments experienced a loss of 21 percent of their workforce capacity over the past decade.
- **Resources are limited**. In 2019, 15 percent of LHDs reported decreased budgets relative to the previous fiscal year, and 52 percent experienced flat funding despite inflation, population growth and increasingly complex public health challenges.
- **Services have been impacted**. As a result of budget and staffing changes, health departments reduced their level of service provision for several services critical to COVID-19 response.

LHDs are on the front lines in the pandemic fight and, as NACCHO says, "chronically underfunded" public health preparedness and response programs make it difficult for them to respond to the crisis. Because the information gathered for this report

Highlights

COVID-19 responsible for most line of duty deaths so far in 2020

NACCHO releases 2019 National Profile of Local Health Departments

PHMSA amends rules allowing transport of bulk methane

Webinars: fire response & unrest; responding to 2 disasters at once

Cyber Threats

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

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.

Disclaimer of Endorsement:
The appearance of external hyperlinks does not constitute endorsement of the linked websites or the information, products or services contained therein. Reference to any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the EMR-ISAC or the U.S. government.

was collected before the pandemic hit, it serves as both a warning and a way to compare services, funding and workforce capabilities in the future.

NACCHO conducts this research every three years. Previous reports can be found on the NACCHO website.

(Source: NACCHO)

PHMSA amends rules allowing transport of bulk methane

The Pipeline and Hazardous Materials Safety Administration (PHMSA) in coordination with the Federal Railroad Administration (FRA), amended the Hazardous Materials Regulations (HMR) allowing for the bulk transport of "methane, refrigerated liquid," commonly known as liquefied natural gas (LNG), in rail tank cars. This rule is effective as of August 24, 2020.

Methane is the primary gas in natural gas. This rulemaking authorizes the transportation of LNG by rail in DOT-113C120W specification rail tank cars with enhanced outer tank requirements, subject to all applicable requirements and certain additional operational controls.

First responders in jurisdictions with rail traffic should be aware of this rule change and review their hazardous materials response procedures related to methane. A good place to start is the Emergency Response Guidebook (ERG), which gives first responders detailed information on hazardous materials to better manage accident or spill response during the critical early stages of an incident. To request a copy of the new 2020 ERG, you must contact your state's ERG distribution coordinator.

The present action is based on a longstanding understanding of the properties of LNG and an evidence-based approach to the safety of the tank cars designed and used to transport flammable cryogenic materials.

(Source: PHMSA)

Webinars: fire response & unrest; responding to 2 disasters at once

Be sure to check out these two topical webinars coming up next week:

When peaceful protests take over the streets and demonstrations turn violent, leading to arson and injuries, fire departments are called to respond alongside law enforcement. These situations create challenging questions about how to fulfill the department mission while protecting firefighters and equipment.

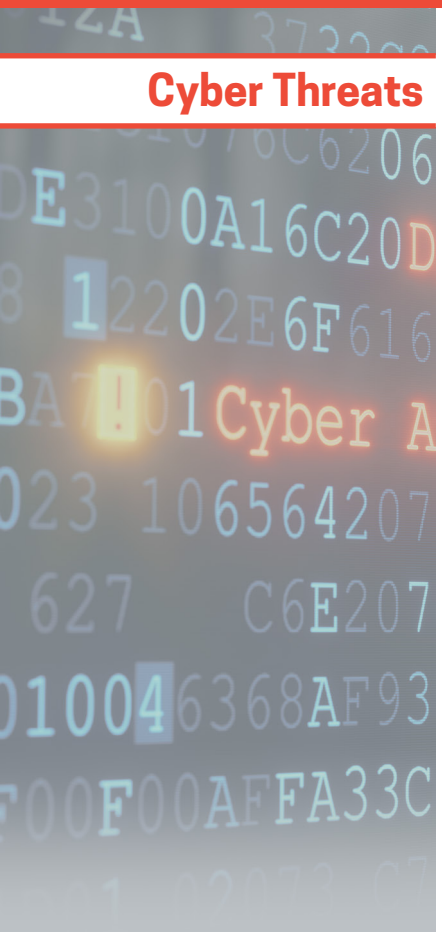
Join Lexipol and the International Association of Fire Chiefs for the webinar Caught in the Middle: Fire Department Response During Civil Unrest on Wednesday, September 16, 2020, at 1 p.m. Eastern. Registration is required.

What does a community do when one day it experiences a mass shooting and the next day it is hit with a devastating tornado? Preparing a comprehensive response to incidents of mass violence or terrorism includes planning for the possibility an incident could occur when a natural disaster or health crisis is taking place. This session covers some of the points to consider when creating a co-response plan.

Join the webinar Developing Co-Response to Mass Violence During a Community Crisis on Wednesday, September 16, 2020, from 2–3:15 p.m. Eastern to learn about how to best plan the possibility of violence occurring at the same time as a natural disaster. Registration is required. This session is offered by the Office for Victims of Crime Training and Technical Assistance Center. The webinar will be recorded.

(Sources: Various)

Cyber Threats



Ransomware Red Flags: 7 Signs You're About to Get Hit

It's every security pro's nightmare: your company has been hit with ransomware, and every machine and server has been encrypted.

Shocked? Likely, but security experts say the warning signs were there all along. Misdirected DNS requests, bad VPN reboots and Active Directory login failures should have been setting off alarms that a ransomware attack was in progress.

It doesn't have to be this way. According to a senior security engineer and malware researcher, mitigation efforts begin with evaluating how vulnerable you are to exploits. For example, are you leaving databases exposed on the public Internet?

And once attackers are in your network, you have anywhere from 48 hours to 12 days before they pull the trigger.

(Source: Dark Reading)

Local government most frequently targeted by ransomware

Local government bodies are more likely to be targeted by ransomware attacks than any other type of organization, according to a new study which looked at 71 global ransomware incidents over the last 12 months.

It found that 44 percent of global ransomware attacks that have taken place so far in 2020 have been aimed at municipalities, which is virtually the same proportion as in 2019 (45 percent).

Of the municipalities subjected to ransomware attacks in 2020, 15 percent confirmed they have made payments, compared to no ransoms being paid last year.

(Source: InfoSecurity Magazine)

US agencies must adopt vulnerability-disclosure policies by 2021

The United States government's cybersecurity agency is now requiring federal agencies to implement vulnerability-disclosure policies, which would give ethical hackers clear guidelines for submitting bugs found in government systems, by March 2021.

Currently, most federal agencies lack a formal mechanism to receive information from white-hat hackers about potential security vulnerabilities on their systems.

The new directive by the Cybersecurity and Infrastructure Security Agency (CISA) aims to change this by requiring agencies to publish policies with detailed descriptions of which systems are in scope, the types of testing that are allowed and how ethical hackers can submit vulnerability reports. A directive is a compulsory direction for federal, executive branch, departments and agencies.

(Source: ThreatPost.com)

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