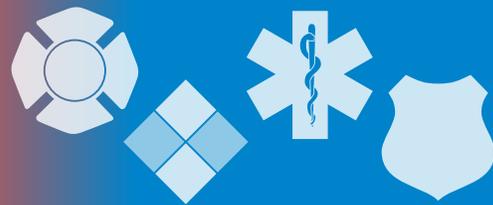


# The InfoGram



Volume 20 — Issue 3 | January 16, 2020

## Wave of struck-by deaths prompts traffic incident safety message

The U.S. Fire Administration (USFA) joins eight other North American fire service organizations in a "[Joint North American Firefighter Survival Message](#)," bringing increased attention to safety at roadway operations following [several struck-by incidents this year resulting in the deaths and injuries of firefighters, law enforcement officers and other responders](#).

According to USFA, 10 percent of firefighter fatalities in 2019 were from struck-by incidents. These kinds of incidents are preventable, but solving the problem will take increased awareness and education - for both the public and first responder personnel.

In the joint message, the International Association of Fire Chiefs (IAFC) shares "[10 Tips For Responding and Operating on Roadway and Highway Incidents](#)" first responders should use to minimize risks. In addition, the organizations involved provide scene safety resources and training for first responders. Links to these resources are at the bottom of the [joint message](#).

It should come as no surprise that distracted driving is increasing, partly due to the use of smartphones and other devices. Departments should strongly consider pushing safety messaging to drivers through social media and regular media. USFA has a [social media graphic available for both Facebook and Twitter](#). ResponderSafety.com offers both [videos and public service announcements](#). See a list of [move over laws for each state and Canadian province](#) on the Automobile Association of America website.

First responder agencies and others who work roadway operations need to be proactive on this issue in order to prevent future struck-by injuries and deaths. Train on known best practices for better scene safety at every roadway incident.

(Source: [IAFC](#))

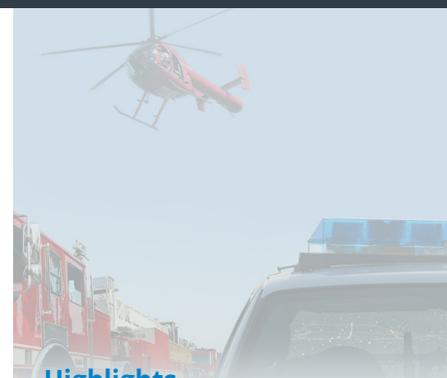
## FEMA releases updated Community Lifelines resources

Lifelines are critical services that enable communities to function. Examples include communications, energy and security. When these [Community Lifelines](#) are disrupted by an emergency or disaster it is crucial to stabilize them as quickly as possible to support the needs of the community during response and recovery.

The Federal Emergency Management Agency (FEMA) released the updated "[Community Lifelines Implementation Toolkit 2.0](#)" and the "[Incident Stabilization Guide](#)." These documents provide updated information and resources so the emergency management community can better understand and implement Community Lifelines.

Since its creation, the lifelines concept has been widely accepted throughout the emergency management community, because the simplicity and plain language used for lifelines eases coordination and communication among partners at multiple levels.

The concept was validated during responses to hurricanes, typhoons, the Alaska earthquake in Anchorage and during the 2019 Shaken Fury full-scale exercise.



### Highlights

Wave of struck-by deaths prompts traffic incident safety message

FEMA releases updated Community Lifelines resources

Update on vaping-related lung injuries from the CDC

Webinar: Communication Partnerships for Public Health Emergencies

### 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](http://www.usfa.dhs.gov/emr-isac) or contact the EMR-ISAC office at: (301) 447-1325 and/or [emr-isac@fema.dhs.gov](mailto:emr-isac@fema.dhs.gov).

[Subscribe here](#)



Lessons learned from these events, as well as stakeholder feedback, are reflected in the Community Lifelines Implementation Toolkit 2.0.

The “Incident Stabilization Guide” explains how FEMA will use the lifelines during response operations and planning and introduces its potential applicability across the preparedness cycle and other mission areas.

(Source: [FEMA](#))

## Update on vaping-related lung injuries from the CDC

In September 2019, the Centers for Disease Control and Prevention (CDC) began reporting on cases of [e-cigarette, or vaping, product use-associated lung injury \(EVALI\)](#). The CDC recently posted an update.

In a new study, evidence points increasingly to an association of EVALI with vaping and e-cigarette products containing tetrahydrocannabinol (THC), as 82 percent of hospitalized patients with data on substance use reported using THC-containing products. Further, 78 percent reported getting the product from informal sources such as friends, dealers or online.

Data acquired from labwork show vitamin E acetate, an additive, is closely related to EVALI as well.

For more information on EVALI and to follow updates, see the CDC’s website.

(Source: [CDC](#))

## Webinar: Communication Partnerships for Public Health Emergencies

Please join the CDC’s Emergency Partners Information Connection on January 29, 2020, at 1 p.m. Eastern for a [webinar on communication partnerships for public health emergencies](#).

In an emergency, how do you share potentially life-saving information with people who are hardest to reach? The answer – sometimes the only answer – is by working with partners who can reach those hard-to-reach populations.

Webinar topics will include how to plan and build these partnerships, how to make partnerships mutually beneficial and how to work with partners to share information with those people who need it most. Webinar participants and viewers will accomplish the following:

- 🔗 Describe the CDC’s role in the topic covered during the presentation.
- 🔗 Describe the topic’s implications for respective constituents.
- 🔗 Discuss concerns and issues related to preparedness for and response to urgent public health threats.
- 🔗 Identify reliable information resources for the topic.
- 🔗 Describe how to promote health improvement, wellness, and disease prevention.

The webinar link, dial-in numbers and other connecting information are available on the CDC website.

(Source: [CDC](#))

### 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.

## Cyber Threats

### Hackers want \$25 million ransom for Texas ransomware attacks

Hackers looking to breach United States computer networks sharply intensified their efforts following the death of Iranian military leader Qasem Soleimani, but have had limited success, according to internet security researchers and state government officials.

Soon after the strike that killed Soleimani, **Iran-based attempts to hack federal, state and local government websites jumped 50 percent** - and then continued to accelerate, said network security company Cloudflare.

Over the course of 48 hours, attacks traced to Iranian IP addresses nearly tripled against targets around the world, Cloudflare said, peaking at half a billion attempts per day.

(Source: [CNN](#))

### Know these common signs of tax season scams

Tax season is in full swing, which means criminals will go to great lengths to separate you from your money, your identity or anything of value within their reach. They may offer seemingly legitimate “tax services” actually designed to steal your identity and your tax refund. Often times, criminals will lure you in with an offer of larger write-offs or refunds. Such scams might include fake websites and tax forms that look like they belong to the Internal Revenue Service (IRS) in order to trick you into providing your personal information.

Due to the rise in data breaches, **you should always take steps to minimize your risk of identity theft and other online-related crimes**; this is especially important this time of the year. See the [Center for Internet Security website](#) for some warning signs to look for and basic precautions you can take to minimize risk and avoid becoming the next victim.

The Internal Revenue Service also compiles the “[Dirty Dozen](#)” list annually. It describes a variety of common scams taxpayers may encounter anytime but many of these schemes peak during filing season as people prepare their returns or hire someone to help with their taxes. See also the “[Taxpayer Guide to Identity Theft](#).”

(Source: [CIS](#) and [IRS](#))

### New Orleans says it will take months to recover from cyber attack

The City of New Orleans says the recent cyber attack on its networks had a more than \$7 million impact, a number the mayor says continues to grow. But, she adds **the city will be able to recover three million of that from a cybersecurity insurance policy** purchased before the attack.

Included in the millions the city will spend to recover from the cyber attack are buying new computers and improving the city’s IT infrastructure and cleaning over 3,400 replacement computers.

The city says sophisticated ransomware was behind the attack but no ransom has been demanded or paid in the last month since it happened.

(Source: [Fox 8 Live](#))

#### Cyber Information and Incident Assistance Links

##### [MS-ISAC](#)

[SOC@cisecurity.org](mailto: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.