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

The InfoGram

Volume 19 — Issue 19 | June 6, 2019

Personally owned vehicles: getting to the scene alive

Every year, firefighters are killed or injured responding to an accident or fire in their privately owned vehicle (POV). Many more firefighters are injured in accidents each year, sometimes with civilian injuries or deaths resulting from multivehicle accidents as well.

State laws vary on the restrictions or immunity granted to volunteers in POVs. In recent years, firefighters have seen jail time and civil cases resulting in fines over $1 million due to POV accidents resulting in civilian fatalities and in some cases departments were sued.

State laws vary on requirements allowing POVs to have lights and sirens. Firefighters should know state laws and regulations and abide by them.

Remember safety starts at the time of the call. Some simple and basic things can mean the difference between life and death:

- Check the map or GPS before leaving for the call, not en route.
- Recognize you are excited. Calm down and don't let it distract your driving.
- Turn off the radio and do not use your cell phone for any purpose while driving.
- Do not assume other drivers notice your lights or siren if you are using them, especially at intersections.
- Do not assume other drivers know safety laws regarding responding POVs.
- If your department does not have a policy for POVs, create one.

Finally, the number one thing you can do for your personal safety is wear your seatbelt. Often, firefighters killed in crashes involving POVs were not wearing seatbelts. All firefighters need to wear seatbelts or restraints every time, no matter if they are responding in apparatus or a POV.

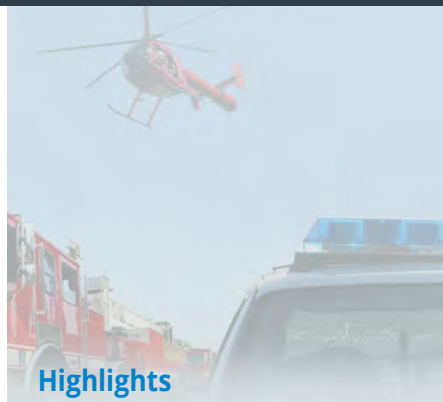
(Source: USFA)

Legal aspects of public health emergencies: online training

The Northwest Center for Public Health Practice (NWCPHP) hosts a free online course focused on the legal uncertainties and restrictions of public health during emergencies. "Legal Aspects of Public Health Emergency Preparedness" provides a summary of legal matters to think about when managing public health and healthcare services in an emergency.

"During emergencies, public health agencies need to know what powers public health officials will have, when they can request assistance from other jurisdictions, and how they will handle volunteers." Public health workers must work within the constraints of managing privacy and civil rights while still performing their job of maintaining public health and safety.

This course is for public health workers and attorneys who work with emergency preparedness programs. Participants will learn:



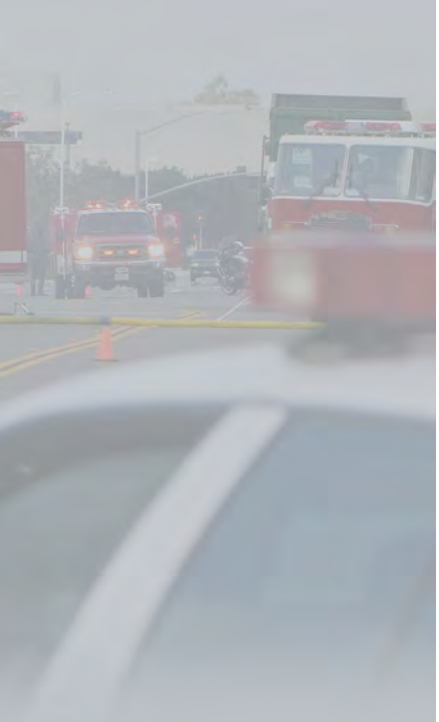
Highlights

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



- How to identify legal authority at different levels of government.
- Understand potential or actual legal powers, responsibilities, and risks during declared emergencies.
- Describe legal questions relating to medical or public health volunteers.

The NWCPHP offers many other courses, webinars, and trainings on their website.

(Source: NWCPHP)

Pocket guide helps responders identify elder abuse

First responders and law enforcement officers often find themselves in positions where they can identify signs of abuse. Child and domestic abuse most quickly come to mind, but elder abuse is a serious problem affecting hundreds of thousands every year.

Approximately 10 percent of Americans age 60+ have experienced some form of abuse, and many agencies responsible for tracking it believe it is underreported. Family members or "trusted others" are most often the abuser.

"Legal Issues Related to Elder Abuse," a pocket guide from the American Bar Association, helps first responders identify the seven types of abuse while providing backup information to help. All types of abuse reportable: physical, sexual, or psychological abuse; neglect; and financial exploitation all qualify as reportable elder abuse. Self-neglect is not a crime, but you can still report it.

The guide covers risk factors to consider; legal topics such as consent, decision-making capacity, and undue influence; abusers; and how a variety of circumstances can be related or relevant to elder abuse issues. Most states have laws requiring people in authority to report abuse, and not reporting it is often a crime.

If you see something that looks fishy but you are not sure, report it. As a responding law enforcement officer or EMS provider, your voice may be the only chance an abused or neglected elder has to escape such a situation.

(Source: American Bar Association)

FEMA introduces new pre-disaster grant program, requests comments

The Federal Emergency Management Agency (FEMA) requests comments on the development and implementation of Disaster Recovery Reform Act (DRRA) Section 1234: National Public Infrastructure Pre-Disaster Hazard Mitigation Grant Program.

This change will allow FEMA to invest in projects that drive risk reduction and build capability for communities and is consistent with the three overarching strategic goals in FEMA's 2018-2022 Strategic Plan. Throughout June, FEMA is hosting a series of four webinars covering various aspects of this new program.

Communities from all levels of government federal, state, local, tribal, and territorial, as well as key stakeholders, including private businesses, citizens, vulnerable and at-risk populations, critical infrastructure sectors, and non-profit, academic, and philanthropic organizations are encouraged to provide comment. The development of the BRIC program – and how as a nation we can deliver those outcomes – is vital.

Comments will be accepted from May 20 through July 15, 2019, on IdeaScale or by email at BUILDBRIC@fema.dhs.gov.

(Source: FEMA)

Cyber Threats

How to write an effective data breach notification

Breached companies might have the obligation to send affected users a breach notification and might have to meet certain content requirements, but too many opt for language and structure that doesn't spur consumers to make use of available protective measures. Researchers recommend devoting more attention to visual attractiveness of the message; making it readable with short sentences and minimal jargon; and avoiding unnecessary information. The article includes an example of a good breach notification.

The researchers also advise law makers and regulators to provide clear guidance on effective data breach notification. That includes specifying what it means to write one in "plain language" and encouraging delivering notifications via multiple channels.

(Source: HelpNetSecurity.com)

Google now letting you automatically delete location, activity history

In early May, **Google introduced a new autodelete feature for location, app and web history**. As opposed to manually having to wipe their histories, with the new feature Google users will be able pick a length of time, either three months or 18 months, that Google will save the data. Any older data will be deleted automatically.

(Source: Cnet)

9-1-1 systems vulnerable to cyber attack

Public-safety answering points (PSAPs) are now well aware of the real-life stories behind the industry's new concern: cybersecurity. In recent years, several **9-1-1 systems have been targeted by hackers**.

Most PSAPs now either have or are planning a move to an IP-based call-answering and call-handling system. These systems come with improved features and functionality. But the benefits come with a responsibility, because IP-based technology can leave NG911 systems open to cyberattacks.

(Source: Urgent Communications)

Extensive flaws in all major building control systems

Building management or automation systems (BMS) or (BAS) are **computer based systems installed in buildings to control and monitor mechanical and electrical equipment such as fire alarms, fire suppression, security, access control,** heating, ventilation, cooling, power and lighting, Over the years the major vendors have built systems that are interoperable with Internet protocols, and some have security flaws hackers can exploit.

What can hackers do with these vulnerabilities? Since Shodan searches show thousands of buildings with these vulnerabilities are connected to the Internet, bad actors can access vulnerable buildings from afar and do things like trigger alarms, lock or unlock doors, control elevator access, intercept video and steal personal information.

(Source: OODAloop)

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.