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

The InfoGram

Volume 20 — Issue 42 | Oct. 15, 2020

Resources to help you protect communities from wildfire

The United States is seeing a very active wildfire season and it shows no signs of slacking off. Responders need all the tools they can to plan response and track incidents in their areas.

InciWeb is a great interactive mapping resource available from the U.S. Forest Service to show where wildfires are burning in areas close to your location, allowing you to better prepare your community for wildfire safety.

It serves as both a trusted reporting tool for public affairs specialists and as a single source of incident-related information for the public. Official announcements include evacuations, road closures, news releases, maps, photographs, and basic information and current situation about the incident.

InciWeb is an interagency all-risk incident information management system. The web-based program provides information for wildland fire emergencies and prescribed fires, but can also be used for other natural disasters and emergency incidents such as earthquakes, floods, hurricanes, tornadoes, and more.

The U.S. Fire Administration's (USFA) Wildland Urban Interface (WUI) webpage offers a collection of resources for you to learn more about wildfire response and management, whole-community involvement and training. This includes information on how to do all these things safely during the pandemic as well as links to other community risk reduction resources.

Follow USFA on Twitter, Facebook and LinkedIn to get the most up-to-date information as it is posted to the USFA website.

(Source: InciWeb and USFA)

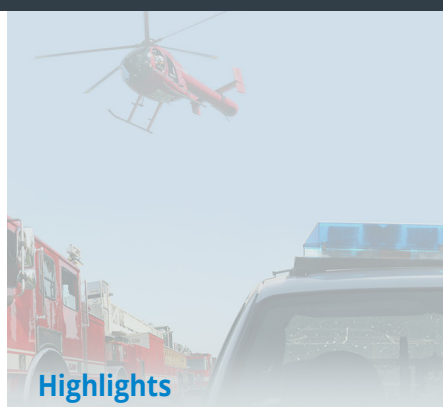
Maintaining Healthcare Safety During the COVID-19 Pandemic

The Technical Resource, Assistance Center, Information Exchange (TRACIE) produced a series of videos to create the collection "Maintaining Healthcare Safety During the COVID-19 Pandemic," now available through its Speaker Series.

Speakers share how their organizations are focusing on healthcare safety during the pandemic and the solutions to system-based issues and concerns. The presentations are for healthcare workers in all settings but focus on hospital-based providers.

Videos cover the following topics:

- The use and operationalization of the Medically Necessary, Time-Sensitive (MeNTS) Procedures tool.
- Implementation of a post-crisis planning committee and the vision for a post-crisis recovery and transformation plan (including a second wave playbook).
- Incorporation of enhanced infection control and prevention strategies, the role of analytics and the use of incident command system for emergency response.
- Application of learning health system concepts to their COVID-19 response including use of real-time internal dashboards.



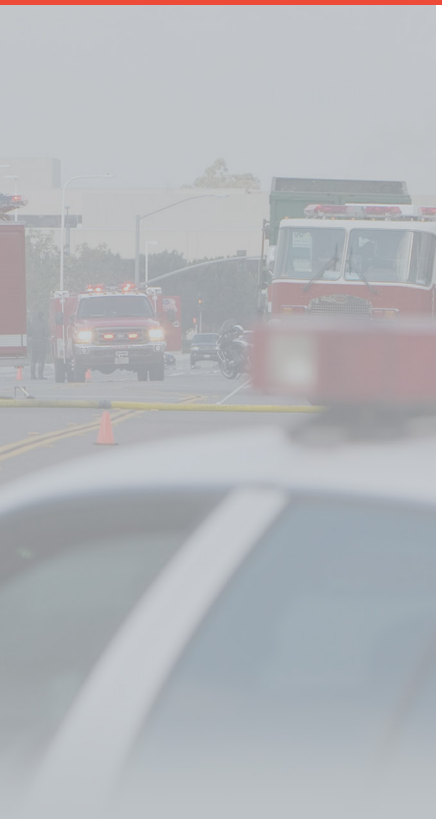
Highlights

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



TRACIE is part of the Department of Health and Human Services Office of the Assistant Secretary for Preparedness and Response (ASPR). ASPR TRACIE maintains a large collection of information related to COVID-19 response, much of which are applicable to pre-hospital response.

(Source: ASPR TRACIE)

FEMA 2020 Hazard Mitigation Assistance Grants period open

The Federal Emergency Management Agency (FEMA) announced the application period is now open for the 2020 Hazard Mitigation Assistance (HMA) grant opportunities:

- Flood Mitigation Assistance (FMA). FMA is available to states, local communities, tribes and territories to reduce or eliminate the risk of repetitive flood damage to buildings and structures insured under the National Flood Insurance Program.
- Building Resilient Infrastructure and Communities (BRIC), a brand new program. BRIC replaces the existing Pre-Disaster Mitigation program and is geared toward incentivizing public infrastructure projects; lifeline risk mitigation; projects incorporating nature-based solutions; and adoption and enforcement of modern building codes.

Eligible applicants must apply for funding through the FEMA Grants Outcomes (GO) system. FEMA GO will replace the legacy Mitigation eGrants system. All applications must be submitted no later than 3 p.m. Eastern on January 29, 2021.

(Source: FEMA)

Webinar: Building Trust for Local Public Health

More than 6 months of pandemic response has strained some working relationships between government agencies, responders, public health, medical facilities and the public. It is crucial to mend any bridges that are showing weakness and head off future problems by identifying what triggered the existing ones.

The October 2020 webinar session of Hot Topics in Practice "Building Trust for Local Public Health," from the Northwest Center for Public Health Practice (NWCPHP), will cover this issue. The director of Idaho's South Central Public Health District will discuss how she builds trust with elected officials, community partners and the public to address the known and unknown health risks associated with the pandemic.

This 1-hour webinar will cover an overview of the health district's unique characteristics, a snapshot of how COVID-19 has impacted the people and industries there, and a discussion of key leadership strategies to manage the politics of the pandemic. The presentation will also list recommendations for supporting staff morale to manage stress and avoid burnout as the pandemic continues.

The webinar is scheduled for Tuesday, Oct, 27, 2020, at 3 p.m. Eastern. Registration is required. Visit the NWCPHP Hot Topics webpage to receive notices about upcoming webinars and to see previous offerings.

(Source: NWCPHP)

Cyber Threats

Everything you need to know about DDoS attacks

A distributed denial-of-service attack (DDoS attack) sees an attacker flooding the network or servers of the victim with a wave of internet traffic so big that their infrastructure is overwhelmed by the number of requests for access, slowing down services or taking them fully offline and preventing legitimate users from accessing the service at all.

While a DDoS attack is one of the least sophisticated categories of cyberattack, it also has the potential to be one of the most disruptive and most powerful by taking websites and digital services offline for significant periods of time that can range from seconds to even weeks at a time.

(Source: zdnet)

How can zero trust help secure the BYOD workforce?

With maximum telework in place for the foreseeable future, federal IT teams are focused on ensuring employees have network access to needed applications and data from any location, on any device. With the quick onset of the pandemic, many agencies were forced to take a bring-your-own-device (BYOD) approach to telework.

The greater variety of endpoints and reduced visibility into these endpoints created even more challenges. BYOD and remote work as a whole complicate agency network infrastructure, increasing the risk of a breach. For example, the operating system on a personal/remote device may not be up to date or its software patched. As federal IT leaders work to accommodate the remote workforce and the resulting added complexity, they are often turning to a zero-trust approach.

With the mantra of "trust no one," a zero-trust architecture is a strategy for managing technology risk. Assessments and grants of trust must happen in a granular fashion. Authorized users receive access to applications – regardless of whether the user is on-site or remote, an agency worker or a third party.

(Source: Government Computer News)

Protecting Connected Cars from Cyberattack

The smart features built into new cars open the door to serious cyber threats. Linked to the internet, connected cars offer cybercriminals the potential ability to remotely access and manipulate the data these systems rely on, which can lead to problems such as exposure of personal information, compromised vehicle security mechanisms or even full control of the vehicle itself.

Innovative automakers, software developers and tech companies are transforming the automotive industry. Drivers today enjoy enhanced entertainment, information options and connection with the outside world. As cars move toward more autonomous capabilities, the stakes are rising in terms of security.

Even if cars are not entirely driverless, their built-in functions are increasingly dependent on applications, connectivity and sensors. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications already allow a car to interact with service providers and infrastructure such as traffic lights. The risks are growing at an alarming rate.

(Source: SecurityBoulevard)

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.