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

The InfoGram

Volume 20 — Issue 9 | February 27, 2020

COVID-19 webinar now available to train EMS and 911 personnel

EMS.gov developed an hour-long training webinar designed as a Coronavirus 2019 (COVID-19) primer for EMS and 911 workers. The multi-agency panel covers the basics of COVID-19, the latest guidance for 911 and EMS, and recommendations for transporting and treating people possibly infected. Accompanying webinar slides are also available (PDF, 6.5 MB).

Details about COVID-19 are changing rapidly and it's easy to get information overload, but first responders need to be prepared to encounter possible cases. The immediate risk to the United States is still considered low; however, the potential public health threat globally and to this country is high.

The webinar recommends initial assessment by 911 telecommunicators. 911 should determine the need for heightened EMS response by screening potential COVID-19 cases for risk factors. If 911 does not provide an initial assessment, EMS is encouraged to conduct the initial assessment at least 6 feet away from the patient.

Use proper PPE consistently when evaluating patients. How COVID-19 is spread is still the topic of investigation. It is presumed to spread the same way other coronaviruses are spread: through person-to-person contact, through droplets from sneezing or coughing, and possibly by touching an object that has the virus on it.

For more information on COVID-19 response and recent developments, see the Centers for Disease Control and Prevention website.

(Source: CDC)

A look at the health impact of wildland fire smoke exposure

Exposure to wildfire smoke may cause more long-term health problems for affected population than originally thought. According to years of research, the particulate matter contained in wildland fire smoke is small enough to reach the bloodstream and spread throughout the body.

Exposure to wildfire smoke may lead to worsening of respiratory conditions, and evidence points to the possibility of wildfire smoke triggering heart-related problems such as heart attacks. These can be mitigated by staying indoors, using proper indoor filters and, if necessary, also using respirators.

Wildland firefighters and their employers should be very concerned about this issue as their exposure is generally much greater than the general population. Researchers are looking at the long-term effects of smoke on wildland firefighters, but data has already shown higher risk of lung cancer and cardiovascular disease.

Wildland fire smoke contains dozens of toxins and carcinogens including carbon monoxide, benzene, formaldehyde, herbicides and silica. Bandanas are not respiratory protection by any standard and do nothing to protect wildland firefighters against these toxins, but use of better respirators are not only restrictive but also can't supply clean air for a 12-hour shift. There is no easy answer to this problem.

To help public health outreach, the Environmental Protection Agency (EPA) maintains a webpage "Smoke-Ready Toolbox for Wildfires" to help public health officials and

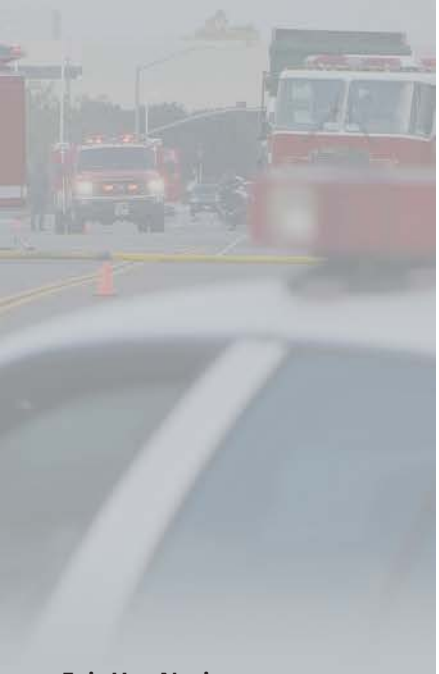
Highlights

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



others understand and manage the risks of smoke exposure.

(Source: EPA)

National Cybersecurity Assessments and Technical Service

With the quickly changing cybersecurity environment, it is difficult to know where to begin, what to focus on or how to keep up. This is especially true for smaller local government agencies with limited resources.

The Cybersecurity and Infrastructure Security Agency (CISA) has cybersecurity services available to federal, state, local agencies, critical infrastructure and private sector organizations. Services of the National Cybersecurity Assessments and Technical Services (NCATS) program include:

- Cyber Hygiene: Vulnerability Scanning
- Phishing Campaign Assessment (PCA)
- Risk and Vulnerability Assessment (RVA)
- Validated Architecture Design Review (VADR)

The first option, Cyber Hygiene: Vulnerability Scanning (PDF, 326 KB), may be the most beneficial place to start. CISA performs regular network and vulnerability scans and delivers a weekly report for your action. The service helps secure your internet-facing systems from weak configuration and known vulnerabilities, and encourages the adoption of modern security best practices.

Once initiated, this service is mostly automated and requires little direct interaction. After receiving the required paperwork for Cyber Hygiene, scans start within 72 hours and you'll begin receiving reports within two weeks.

See a sample Cyber Hygiene report on the NCATS website. Request information about the service(s) you are interested in by emailing ncats_info@hq.dhs.gov.

(Source: CISA)

Webinar: tactical EMS program considerations

During shooting incidents, experience shows lives are saved if medical teams can access victims as soon as possible. Allowing tactical paramedics to make entry with SWAT and law enforcement tactical units is becoming increasingly more popular around the world, resulting in the creation of Tactical EMS (TEMS) teams.

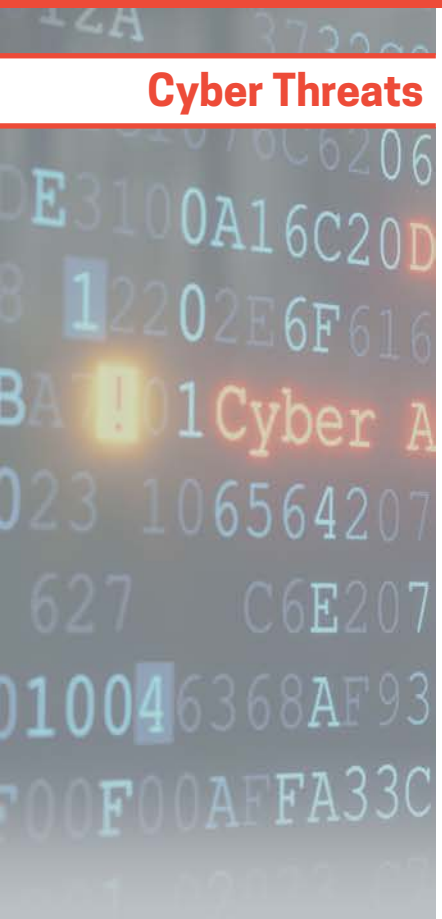
Join the webinar "TEMS Scope of Practice and Policy Considerations Panel" to learn more about creating a TEMS program in your jurisdiction. During this webinar, attendees will hear from TEMS practitioner, subject matter experts from the International Public Safety Association's TEMS Committee

TEMS teams are trained to accept more risk and learn how to mitigate certain risks by adjusting the type of care provided (e.g., assess whether to provide rapid hemorrhage control and then move a patient, or whether to move the patient from the crisis point before providing medical care). The dynamic environment, threat and form of care is not new to the TEMS provider.

This webinar is scheduled for Wednesday, March 4, 2020, from 1-2:15 p.m. Eastern. Registration is required, connection information will be sent to registrants.

(Source: IPSA)

Cyber Threats



FBI recommends passphrases over password complexity

For more than a decade now, security experts have had discussions about what's the best way of choosing passwords for online accounts.

There's one camp that argues for password complexity by adding numbers, uppercase letters and special characters, and then there's the other camp, arguing for password length by making passwords longer.

Last week in its weekly tech advice column known as Tech Tuesday, the FBI Portland office positioned itself on the side of longer passwords.

The idea behind the FBI's advice is that a **longer passphrases, even if relying on simpler words and no special characters, will take longer to crack and require more computational resources**.

The FBI's advice echoes a now-infamous XKCD webcomic that made the concept of passphrases-over-passwords widely known among internet users.

(Source: zdnet)

Emotet threat far from over

In a troubling development for organizations, security researchers report a recent **resurgence in activity related to Emotet** — malware that the Department of Homeland Security (DHS) has previously described as among the most destructive ever.

Cisco Talos on Thursday reported seeing increased Emotet activity targeting military domains and domains belonging to state and federal governments.

According to the vendor, the operators of Emotet appear to have successfully compromised accounts of one or more people working for or with the government and sent out spam emails containing the malware to their contacts. The result was a rapid increase in the volume of messages containing Emotet directed at .mil and .gov top-level domains last month and so far this month.

(Source: DarkReadings)

Connect with CISA on Facebook to keep up with cyber news

The Cybersecurity and Infrastructure Security Agency (CISA) is expanding its external reach to a new platform: Facebook.

As a new agency with a collaborative mission, **CISA's success depends upon the ability to communicate with partners and the public**. Facebook will be a critical platform to share resources, make announcements and encourage followers to be proactive about managing risk.

CISA now maintains a presence on four social media platforms: Facebook, Twitter, LinkedIn, and YouTube. Please like, follow, and connect with CISA's social media feeds.

(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.