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

The InfoGram

Volume 20 — Issue 26 | June 25, 2020

Emergency Services Sector Active Shooter Guide

Active shooter incidents are low- or no-notice events and can happen anywhere. In its report, the FBI reported 28 active shooter incidents in 2019 injuring or killing 247 people. Incidents are recorded in schools, hospitals, houses of worship, places of employment and open areas. They happened in both small towns and large metropolitan areas.

No community is immune, as the recently released Emergency Services Sector Active Shooter Guide points out. Produced by the Department of Homeland Security's (DHS) Emergency Services Sector Specific Agency, the tri-fold guide walks first responder departments through the four-step process of developing an active shooter program:

- Awareness. Maintain a sense of organizational awareness of this issue and know where you can find resources (FBI, DHS, etc.).
- Training. Improve local active shooter planning and preparedness through no-cost online training. The guide provides links to some training.
- Community Outreach. Make collaborative networks within your community. Not only will this help during an actual incident, but people are more likely to report suspicious activity to a friendly face within the public safety community.
- Exercise Coordination. Exercises can identify training and planning gaps, and they are an excellent opportunity to build the three previous bullet points.

DHS lists resources for all the steps in this program. In addition, see its Active Shooter Emergency Action Plan Guide and Template and its webpage dedicated to Active Shooter Preparedness resources.

(Source: DHS)

COVID-19 cases spike, hit record high numbers this week

On Wednesday, the United States recorded over 45,500 new case of COVID-19, breaking the daily record of newly reported cases of COVID-19 by over 9,000 cases previously set in April. This tracks with world numbers – the World Health Organization reported a record of 183,000 new cases worldwide on Sunday.

Many lawmakers are currently saying they will not reinstitute restrictions and closures which kept people home, and many people are not adhering to current measures intended to limit the spread of the virus. Experts say the current spike can be traced to Memorial Day weekend gatherings and celebrations.

With another holiday coming up, we may see more of the same regardless of consequences. So, it is unlikely cases will go down and they could continue to rise. The increased load on our medical system – including EMS – may not let up for some time.

In addition, the Centers for Disease Control and Prevention estimates 130,000-150,000 related deaths in the United States by July 18, 2020, and 180,000 by October.

It is increasingly important EMS departments confront issues that have surfaced

Highlights

Emergency Services Sector Active Shooter Guide

COVID-19 cases spike, hit record high numbers this week

Webinar: 911 DataPath provides framework for future needs

National Fire Academy application deadline approaching

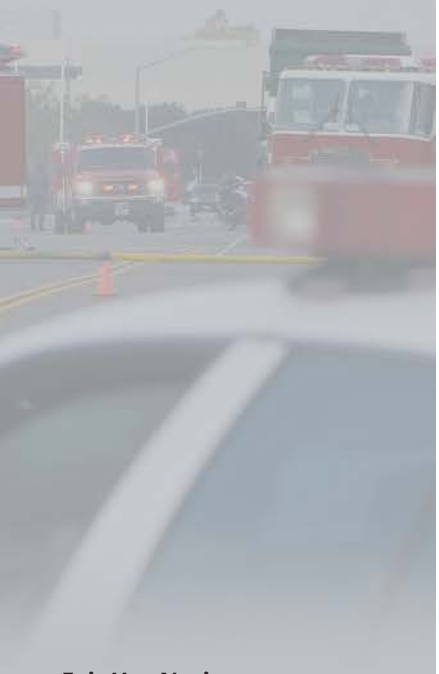
Cyber Threats

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



in the past few months: ensure your supply chain and stock up on PPE and other medical equipment; monitor and address signs of fatigue and stress within your workforce; and review and update plans, policies and procedures to make the workload smoother and easier to bear.

Resources are available through the U.S. Fire Administration, CDC, EMS.gov and the Federal Emergency Management Agency.

(Sources: Various)

Webinar: 911 DataPath provides framework for future needs

The next State of 911 webinars will cover the 911 DataPath, an initiative to produce a framework to enable the voluntary adoption of a uniform 911 data system.

PSAPs and Emergency Communication Centers (ECCs) focus on helping those in need and saving lives. In order to do this effectively, 911 relies on data and information sharing, both locally and nationally. A standard 911 data system doesn't exist so the opportunity to share actionable data across the nation is limited.

Stakeholders in the 911 community are coming together to begin identifying important data points and a common way to reference them. This will help improve operations, support data needs to secure funding and continue to standardize progress toward NG911.

The 911 DataPath initiative is underway and needs input on the types of administrative data for decision making that would be useful when shared with other 911 systems. In this webinar, initiative participants and the National 911 Program will address:

- How access to timely, automated, reliable data sharing will help PSAPs and ECCs in their everyday work.
- How the 911 community can learn about and contribute to this effort to ensure it best meets the needs of all 911 systems.
- The types of data under consideration as the initial task of this data collection and sharing effort.

Register for one of the two upcoming webinars on July 7, 2020, and July 14, 2020. Also be sure to subscribe to be notified of future webinars. See the 911.gov website for recordings of past webinars.

(Source: 911.gov)

National Fire Academy application deadline approaching

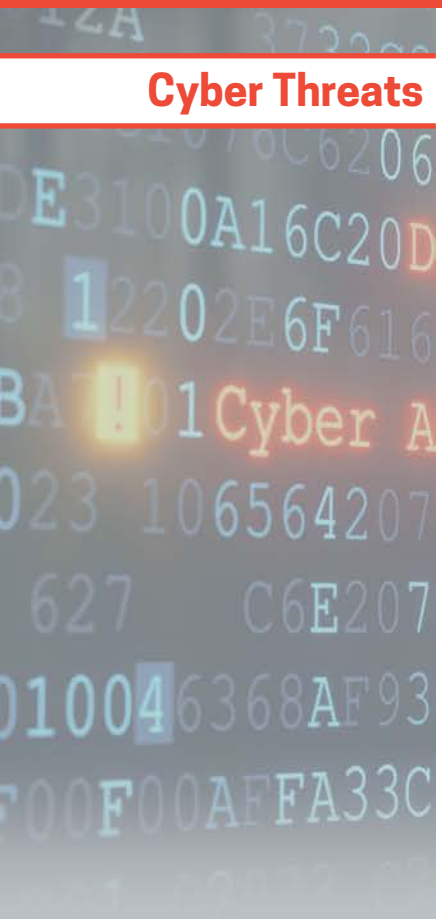
The application period for the National Fire Academy's October 1, 2020-March 31, 2021 semester closes this coming Tuesday, June 30, 2020. There is still time to get in your application.

After choosing a course and making sure you meet the course requirements, you may apply online. You must have a Student Identification Number (SID), and you must submit all application materials at the same time. You will not be able to submit more documentation at a later date.

See the USFA website for detailed instructions, a link to apply for a SID, and a full list of available courses.

(Source: USFA)

Cyber Threats



Data from 200 US police departments, fusion centers published online

An activist group has published 296GB of data they claim was stolen from United States law enforcement agencies and fusion centers.

The files, dubbed BlueLeaks, have been published by Distributed Denial of Secrets (DDoSecrets), a group that describes itself as a "transparency collective."

The data has been made available online on a searchable portal. According to the BlueLeaks portal, the leaked data contains more than one million files, such as scanned documents, videos, emails, audio files and more.

DDoSecrets claims the leaked files contain more than ten years-worth of files belonging to more than 200 police departments and law enforcement fusion centers.

According to DDoSecrets, most of the files are police and FBI reports, security bulletins, law enforcement guides and more. Some of the files also supposedly contain sensitive and personal information, such as names, bank account numbers, and phone numbers.

(Source: zdnet)

Free security resources for those working from home

As the world "shelters in place" amid the COVID-19 crisis, some tech companies are stepping up and offering their products and services free of charge for a limited time. These offers will help organizations set up and protect remote employees faster. In some cases, vendors are also offering support services to help companies through the set-up and deployment processes.

Keep in mind that most if not all these offers are extended free trials. At some point, you will be expected to pay for these products and services if you decide to continue using them. Even so, the vendors listed are helping the global community better cope with the COVID-19 crisis at a time of very high demand for their offering

(Source: CSOonline)

Ransomware operators lurk on your network after their attack

Once ransomware is deployed, many victims have told BleepingComputer that while their network is still compromised, they think the ransomware operators are now gone from the system. This belief is far from the truth, as illustrated by a recent attack by the Maze Ransomware operators.

This breach occurs through exposed remote desktop services, vulnerabilities in VPN software, or via remote access given by malware. Once they gain access, they use tools to gather login credentials and spread laterally throughout the network.

They then use these credentials to steal unencrypted files from backup devices and servers before deploying the ransomware attack.

(Source: Bleeping Computer)

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