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

The InfoGram

Volume 20 — Issue 7 | February 13, 2020

CDC releases interim coronavirus guidance for EMS and 911

This week the Centers for Disease Control and Prevention (CDC) published "Interim Guidance for Emergency Medical Services (EMS) Systems and 911 Public Safety Answering Points (PSAPs) for 2019-nCoV in the United States."

The CDC recommends 911 and emergency medical dispatch screen callers for signs, symptoms and risk factors of 2019 Novel Coronavirus (COVID-19). Dispatch should report potential COVID-19 cases to EMS before their arrival. EMS can evaluate individuals and transport them as a Person Under Investigation if necessary.

The interim guidance suggests specific modifications to EMS practices for patient assessment, PPE use and aerosol-generating procedures (e.g., intubation, CPR, etc.). They discuss transporting patients, documentation of patient care, cleaning transport vehicles and recommends using the "EMS Infectious Disease Playbook" (PDF, 1.1 MB) as a good resource.

The CDC also touches on EMS employer responsibilities and describes the interim guidance as a way for employers to assess current practices, procedures and training to ensure they are all up-to-date. This sections talks about donning and doffing PPE, task-specific training and education, use of respiratory devices, and ensuring you have adequate supplies and well-trained decontamination staff.

Both PSAP and EMS departments responding to patients at ports of entry or airports that are CDC-designated quarantine stations should be in contact with the local CDC quarantine station staff and let them know of potential cases. It is a good idea to familiarize your staff with the CDC's interim guidance and make contact with the quarantine station before you need them.

The World Health Organization (WHO) produced an online course intended for public health professionals, incident managers and personnel working on the COVID-19. It is available through the WHO's online open learning platform for emergencies. Registration is required; see the short introductory video for an overview.

(Source: CDC)

Upcoming changes to FEMA's National Exercise Program

The Federal Emergency Management Agency (FEMA) provides assistance for exercise design, development, conduct and evaluation at no cost to whole community partners through the National Exercise Program (NEP). Beginning in March 2020, FEMA is changing the nomination process sponsors use to request exercise support through the NEP by supporting jurisdictions most in need and addressing capabilities most important to them.

In the new process, FEMA will only review nomination forms and respond to requests for exercise support twice a year. The deadline for submitting to the Spring 2020 Nomination Round is March 31, 2020, with decisions issued by May 1, 2020. Submissions will not be reviewed outside of the established nomination rounds listed on the NEP website.

All exercise support requests received will be considered; however, support is dependent on resource availability and program fit. When reviewing nominations,

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

FEMA looks for support requests that:

- Align to at least one of the 2019-2020 Principal's Strategic Priorities (PDF, 295 KB).
- Engage a broad spectrum of participants (e.g., private sector and non-profit partners).
- Use the exercise to examine existing plans or validate corrective actions from previous exercises or real-world events.
- Address capability gaps in assessments such as the Stakeholder Preparedness Review.

To assist our partners in preparing nominations, FEMA will host a series of webinars that will include an overview of upcoming changes, discuss the benefits of nominating an exercise to the NEP and answer any questions. Webinar dates and times:

- Wednesday, February 19, 2020, at 1:00 p.m. Eastern.
- Thursday, February 20, 2020, at 3:00 p.m. Eastern.
- Wednesday, February 26, 2020, at 9:00 p.m. Eastern.

Please join via the webinar link https://fema.connectsolutions.com/NEPoverview to follow along with the slides; audio will only be available through the conference line: 1-800-320-4330, pin 559550. The content for each of the webinars will be the same. If you have any questions, please reach out to NEP@fema.dhs.gov.

(Source: FEMA)

FBI releases 2000-2018 Active Shooter Incidents Topical One-Pagers

The FBI just released a set of one-page sheets detailing active shooter incidents between 2000-2018. Each page concentrates on one aspect of these incidents, such as Casualty Breakdown or Incident Locations, giving law enforcement officers, first responders, businesses, educators and the general public a better understanding of related statistics.

Between 2000-2018, the FBI identified 277 active shooter incidents in the United States with 282 shooters. In those incidents, there were 2,430 casualties (884 killed and 1,546 wounded). Law enforcement personnel made up 104 of the total casualties, the rest were civilians.

See the individual one-page sheets for more detailed statistics. Some numbers of interest to first responders, venue and business owners and other stakeholders:

- Shooters are most likely to be apprehended by law enforcement. Shooter suicide comes in a close second.
- Most incidents happen in commerce areas, followed by educational settings.
- Only four incidents out of 277 had multiple shooters.

The FBI notes a possible shift in shooter outcome. The number of shooter suicides and shooters killed have gone down in the past few years while apprehensions by law enforcement have increased.

(Source: FBI)

Cyber Threats

CISA releases Elections Cyber Tabletop in a Box

The Cybersecurity and Infrastructure Security Agency (CISA) developed the **Elections Cyber Tabletop Exercise Package as a resource for state, local, and private sector partners** (commonly referred to as "tabletop in a box"). The package includes template exercise objectives, scenario, and discussion questions, as well as a collection of cybersecurity references and resources.

Partners can use the exercise package to initiate discussions within their organizations about their ability to address the potential threats to the election infrastructure. An editable Word version of the Elections Cyber Tabletop Exercise Package can be requested by email; the PDF version is available on the CISA website. Contact cisa.exercise@cisa.dhs.gov.

(Source: CISA)

Cryptocurrency-mining bot found on Department of Defense network

A security researcher hunting for bug bounties discovered last month that **a cryptocurrency-mining botnet had found a home and burrowed inside a web server operated by the United States Department of Defense** (DOD).

Initially, the bug report was filed in relation to a misconfigured automation server running on an Amazon Web Services server associated with a DOD domain. Full access was apparently possible, including to the filesystem.

(Source: zdnet)

Some ransomware hackers take the money and run

A survey by researchers found that 33 percent of organizations infected with ransomware opted to pay the ransom.

But some **22 percent of those who paid a ransom said they never got access to their data locked up by the malware**, and nine percent said they got hit with additional ransom demands after paying.

(Source: Security Week)

ODNI to share more cyber threats in new counterintelligence strategy

The Office of the Director of National Intelligence (ODNI) will take a "whole of society" approach that hopes to **encourage greater private-sector participation in protecting the country from cyber threats**, according to a leading official. The National Counterintelligence Strategy was released on Monday.

The director of ODNI's National Counterintelligence and Security Center's announcement is in line with pledges by government agencies such as the Cybersecurity and Infrastructure Security Agency and the National Security Agency to share more contextual information about cyber threats – without sharing classified sources or methods – with industry.

(Source: NextGov)

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