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

The InfoGram

Volume 19 — Issue 43 | November 21, 2019

EMS Compass 2019 revision released

Initially released in 2016, the EMS Compass is a set of 14 quality measures EMS stakeholders can use to evaluate performance and improve systems of care.

The EMS Compass was recently revised by the National EMS Quality Alliance (NEMSQA). The August 2019 revision updates 11 of the 14 proposed measures of care within the topics of Hypoglycemia, Pediatrics, Seizure, Stroke, Trauma, and Safety. Quality measures look at clinical process, patient experience and patient safety within these topics.

EMS Compass is intended to be a guide but is not a standard or requirement and is not intended to measure every aspect of EMS performance. NEMSQA plans to use feedback provided by EMS stakeholders to improve on the measure set in the future.

To support the 11 measures, NEMSQA also offers flowcharts, worksheets, frequently asked questions and a specification table. In addition, they provide electronic specifications for information technology departments with measure implementation and data extraction.

Funded by the National Highway Traffic Safety Administration, EMS Compass was originally developed by the National Association of State EMS Officials (NASEMSO). The American College of Emergency Physicians took over the contract in 2017, and now the contract is managed by the NEMSQA.

(Source: NEMSQA)

FEMA updates Procurement Disaster Assistance Team Field Manual

During the response and recovery of a disaster is the worst time for communities to realize they don't know the process for requesting public assistance from the Federal Emergency Management Agency (FEMA). Communities should be familiar with regulations and rules before it is needed.

FEMA released an updated field manual on procurement processes after a disaster (PDF, 1.2 MB). The manual supports FEMA staff in providing accurate and consistent information to Public Assistance applicants on how to comply with the federal procurement under grant requirements.

This version of the manual merges and streamlines relevant content from two previous editions. It has internal clickable hyperlinks to take readers to applicable resources, and is structured along the lines of the progression of federal procurement.

The information in the manual applies to procurements under disasters declared on or after December 26, 2014. Additional resources to support compliance requirements when procuring with federal grant funds are available on the FEMA website.

(Source: FEMA)

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

Real Estate ISAC bridges the public-private partnership gap

There is growing terrorist and domestic extremist interest in commercial facilities as a target of interest, as they are a gathering place for people. First responder coordination with venue or commercial security and management is more important than ever when planning exercises, writing emergency plans and procedures, or responding to an incident.

The Real Estate Information Sharing and Analysis Center (RE-ISAC) promotes cross-sector coordination, something becoming much more important to the Emergency Services Sector. The RE-ISAC assists commercial facilities to meet these threats through daily information sharing and analysis on current threats and identified vulnerabilities.

The RE-ISAC's role is to enhance the security and resilience of the commercial real estate sector, identified as a national critical infrastructure. Created by Presidential Policy Directive 21, the RE-ISAC provides members with information on terrorism, physical and cyber security, and natural hazards warning and response to the sector.

The Commercial Facilities Sector comprises:

- Lodging - hotels, motels and resorts.
- Entertainment and media - movie studios, broadcast media.
- Retail - retail centers and districts, shopping malls.
- Gaming - casinos.
- Outdoor events and public assembly - amusement parks, fairs, parades and campgrounds, arenas, stadiums, zoos, museums and convention centers.
- Real estate - office and apartment builidngs, mixed-use facilities, self-storage.
- Sports leagues - professional sports leagues and federations.

Those who fit into the Commercial Facilities Sector can find membership information and more details on services on the RE-ISAC website.

(Source: RE-ISAC)

Webinar: Public Safety Drone Programs: A Multidiscipline Approach

Unmanned Aerial Systems (UAS, commonly called drones) have a lot to offer law enforcement agencies, fire departments and emergency management offices, but the operational costs involved with purchasing, maintenance and training may be too much to bear alone.

Have you considered teaming up? A multidiscipline public safety drone program offers the ability to share the burdens of operational costs, drone purchases, training and remote pilots. Learn how this approach might benefit your department.

The International Public Safety Association (IPSA) is holding a free webinar covering this topic on Wednesday, December 4, 2019 from 1-2:15 p.m. Eastern. Registration is required for attendance.

(Source: IPSA)

Cyber Threats

Researchers hack home assistant devices by shining lasers at them

Siri, Alexa and Google Assistant are vulnerable to attacks using lasers to inject inaudible – and sometimes invisible – commands into the devices and **surreptitiously cause them to unlock doors, visit websites, and locate, unlock, and start vehicles**. The attack works against Facebook Portal and a variety of phones.

As voice-controlled systems often don't require users to authenticate themselves, attacks can be carried out without the need of a password or PIN. Even if the systems require authentication for certain actions, it may be feasible to brute force a PIN as many devices don't limit the number of guesses a user can make.

Among other things, light-based commands can be sent from one building to another and penetrate glass when a vulnerable device is kept near a closed window.

(Source: Ars Technica)

Iranian hacking group prompts warning from U.S. Cyber Command

The Iranian hacking group behind a Microsoft Outlook attack earlier this year that prompted a United States Cyber Command warning is back in the news. The United States warned of an increasing threat from Iran as tensions escalate in the Gulf.

Iran doesn't have the same level of cyber weaponry used by threat groups in Russia and China, but it has **proven very adept at attacks on civilian and critical infrastructure** – targets that are less hardened than government or military agencies. Now a report has exposed the use of a dedicated virtual private network by one Iranian hacking group to hit targets while keeping its activities secret.

(Source: Forbes)

Malware attacks on hospitals about to get a lot worse

Trojan malware attacks targeting hospitals and the healthcare industry rose significantly over the course of this year as hackers increasingly look to exploit a sector often viewed as an easy target.

Figures in The State of Healthcare Cybersecurity report from Malwarebytes say there's already been a **60 percent increase in trojan malware detections in the first nine months of 2019** compared with the entirety of 2018. The rise has been particularly significant in the third quarter of this year, with an 82 percent increase in detections when compared with the previous quarter.

(Source: zdnet)

Hacked Disney+ accounts on sale for $1

Disney's new video-on-demand streaming service has been compromised within a week of its being launched, with **hacked Disney+ accounts offered for sale online for just $1**.

Exacerbating the problem is the fact that the Disney+ service has been set up in just the manner you'd expect from a company that pedals the idea of "happily ever after." For each account, connection to a maximum of ten devices is permitted, and there is currently no way to remove any devices that have been connected.

(Source: Infosecurity Magazine)

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.