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

The InfoGram

Volume 19 — Issue 23 | July 5, 2019

Learn about your fire department's survival culture

A fire department's safety culture is a strong predictor of firefighter injuries or deaths. Leadership can improve staff behaviors by placing a stronger value on safety, but you really need to know where you are before you know what to improve.

The Fire Department Safety Officers Association and Drexel University's Center for Firefighter Injury Research & Safety Trends partnered to create the Fire Service Organizational Culture of Safety (FOCUS), a tool to measure your departments safety culture.

Over 400 fire departments in the United States have already taken advantage of this free tool. Departments that take part will receive:

- Customized data of your safety culture at both the department and station levels.
- A comparative analysis of your safety culture to other similar departments.
- Objective evidence to inform safety related policy decisions.

The FOCUS assessment tool is now on version 2.0 and is now funded through August 2020. The program office recommends departments assess their safety culture as soon as possible. One entry per department will be accepted. All information is confidential and will only be shared with your department's point of contact.

(Source: Drexel University)

New Nationwide SAR Initiative website

On June 30, 2019, all information and training located on the former Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) website was transitioned to the new NSI website at the Department of Homeland Security. The new NSI website will be sole host of the online NSI SAR training videos.

This new site provides the same information, resources and training held within the previous NSI website but with easier navigation. The website offers information about the NSI program and a variety of online resources related to the NSI and information and links to partner organizations at the federal, state, local and tribal levels.

NSI video training provides Suspicious Activity Reporting for line officers, fire/EMS, public health and healthcare partners, emergency managers, 9-1-1 personnel and hometown security partners. Each of the sector-specific SAR trainings discuss how to report suspicious activity to the proper authorities while maintaining the protection of citizens' privacy, civil rights and civil liberties.

NSI is in the process of updating outreach materials with the new website; however, please continue to use NSI reference and outreach material which may include the previous web address, as all visitors will be redirected to the new website. If you have any questions, please feel free to contact NTER@hq.dhs.gov.

(Source: Nationwide SAR Initiative)

Highlights

Learn about your fire department's survival culture

New Nationwide SAR Initiative website

FEMA seeks feedback on 2013 HSEEP refresh

Webinar: Using Supplemental 911 Location Data to Improve Response

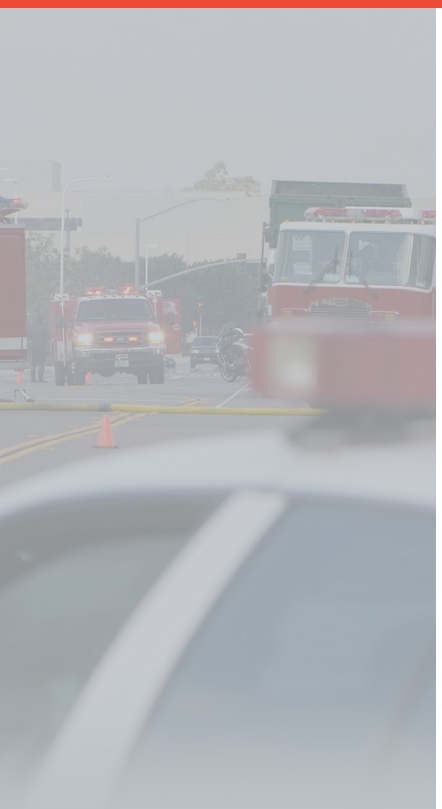
Cyber Threats

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



FEMA seeks feedback on 2013 HSEEP refresh

The Federal Emergency Management Agency (FEMA) began an open review of the 2013 Homeland Security Exercise and Evaluation Program (HSEEP) doctrine this week. FEMA seeks to incorporate lessons learned and best practices from the past six years of HSEEP's use among the whole community's exercise practitioners.

Initial outreach and engagement runs July 1 through August 15, 2019. Feedback/suggestion will be accepted through August 15 at: HSEEP@fema.dhs.gov. Secondary outreach and engagement based on initial inputs is slated for October 1-21, 2019.

A critical element of the HSEEP review process is direct engagement with state, local, tribal, territorial and Federal partners and stakeholders. FEMA will conduct a series of one-hour webinars open to all stakeholders. Webinars currently scheduled:

- Monday, July 8, 2019 at 4:00 p.m. Eastern.
- Wednesday, July 10, 2019 at 1:00 p.m. Eastern.
- Friday, July 12, 2019 at 9:00 a.m. Eastern.
- Monday, July 22, 2019 at 4:00 p.m. Eastern.
- Wednesday, July 24, 2019 at 1:00 p.m. Eastern.
- Friday, July 26, 2019 at 9:00 a.m. Eastern.

No pre-registration is necessary. Webinars are held through Adobe Connect. The call-in number is 1-800-320-4330; PIN 504024#.

Through HSEEP, exercise program managers can develop, execute and evaluate exercises addressing priorities established by an organizations' leaders. The use of HSEEP – in line with the National Preparedness Goal and the National Preparedness System – supports efforts across the whole community, improving our national capacity to build, sustain and deliver core capabilities.

(Source: FEMA)

Webinar: Using Supplemental 911 Location Data to Improve Response

A 911 caller's location is considered the most critical piece of information required to properly route the call and provide emergency response in a timely fashion. Location information will continue to improve as technology and emergency communications improve, but what is available today?

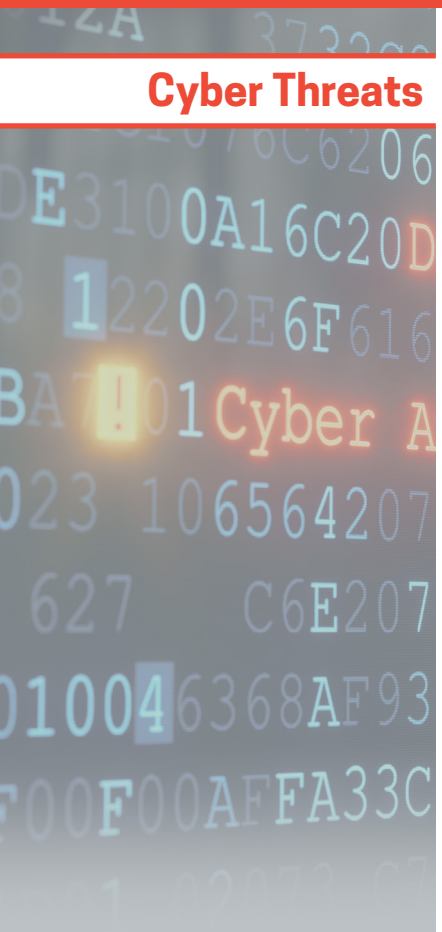
911.gov is hosting the webinar "Using Supplemental 911 Location Data to Improve Emergency Response" on Tuesday, July 9, 2019 at noon Eastern. It will cover supplemental location tools available now and how they help 911 better locate callers. One such tool is the "Recommended Best Practices Guide for Supplemental 911 Location Data" (PDF, 7.9 MB) that:

- Describes how supplemental 911 location data is provided to PSAPs.
- Compares those processes to the way location information is provided by traditional 911 call processes.
- Recommends a set of best practices to guide the development, delivery and use of supplemental 911 location data.

Registration is required. Past "State of 911" webinars are archived on the 911.gov website and are available for viewing.

(Source: 911.gov)

Cyber Threats



Emergency Alert System vulnerable to hacking

In 2018, an emergency alert sent to local phones informed Hawaii residents of an impending nuclear ballistic missile attack, triggering some understandable panic. Needless to say, the attack wasn't real, and a subsequent investigation found that the bogus alert was the result of little more than a clerical error.

But the event prompted researchers at the University of Colorado Boulder to ask the question: **How easy would it be to exploit the nation's emergency alert systems**? What they found isn't particularly comforting.

(Source: Vice)

How organizations can better defend against DNS attacks

Domain Name System (DNS) attacks target many industries, each with certain consequences. Government saw the highest level of theft of sensitive information, and utilities suffered the highest costs from such attacks, according to a recent report. **What's needed is a more proactive approach to prevent or predict attacks before they occur**, or at least before they can cause significant damage.

(Source: TechRepublic)

Healthcare Industry Cybersecurity Workforce Guide

The Healthcare Industry Cybersecurity (HCIC) Task Force's **workforce-oriented cybersecurity recommendations** include:

- Identifying cybersecurity leadership's role for driving robust policies, processes and functions with clear engagement from executives.
- Establishing models for resourcing the cybersecurity workforce with qualified individuals.
- Creating Managed Security Service Provider models to support small and medium-sized healthcare providers.
- Evaluating options for small and medium-sized providers to migrate patient records and legacy systems to secure environments.

(Source: Health Sector Coordinating Council)

The Ransomware Hostage Rescue Guide webcast

It is estimated that a business falls victim to a ransomware attack every 40 seconds, adding up to a projected $11.5 billion in damages for this year. As ransomware attacks become more targeted and damaging, **your organization faces an increased risk of having networks down for days or even weeks**.

This webcast will look at features of new ransomware strains, give actionable info that you need to prevent infections and provide tips on what to do when you are hit with ransomware. This webcast will cover: how to determine if your systems are infected and what to do if they are; proven methods of protecting your organization; and how to create a "human firewall."

(Source: MCPmag.com)

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.