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

The InfoGram

Volume 19 — Issue 24 | July 11, 2019

Improving fire department relevance, visibility in the community

Keeping a high level of visibility within your community is crucial to the growth and sometimes even to the survival of your fire department - especially volunteer or combination departments.

There are several ways to improve your visibility. Good signage, digital signs promoting departmental events or training and flags all signal the locations of departments. This provides subtle and regular reminders of the department's location. Simple as it may sound, this may save many lives over the years as walk-ins show up at stations without warning for medical treatment or during emergencies.

Nothing promotes visibility as well as good community involvement. Open houses, booths at local fairs, carnivals, tours of the station or apparatus visits to schools give community members a name and face to connect with the department. They also provide opportunities to answer questions, explain the what's and why's of the work you do, and can be excellent recruitment events.

Community involvement does not have to only be about your jobs or official duties. Many stories have surfaced in recent years of crews finishing the mowing of a heat exhaustion victim they just transported or cleaning up some vandalism. These feel-good stories get noticed, show you care about your community and all the people in it, and have a secondary benefit of being good public relations.

(Source: FireRescue1)

DHS program gives emergency communications the priority

The Telecommunications Service Priority (TSP) is a multi-faceted program authorizing national security and emergency preparedness (NS/EP) organizations to receive priority treatment for vital voice and data circuits.

NS/EP services are those used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property or degrades or threatens the NS/EP posture of the United States.

The TSP program authorizes priority treatment for interstate, intrastate, foreign communications systems as well as services provided by government and non-common carriers.

TSP provides several training videos on the program and its various parts. For more information on the TSP program, eligibility and frequently asked questions, visit the TSP page hosted by the Cybersecurity and Infrastructure Security Agency.

(Source: CISA)

National Health Security Preparedness Index 2019

The 2019 National Health Security Preparedness Index (NHSPI) shows the United States scores a 6.7 on a 10-point scale for preparedness. That's a 3.1 percent improvement over the 2018 Index and 11.7 percent improvement since the Index began in 2013. The overall growth is good, but work is obvioiusly needed.

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

The 2019 NHSPI (PDF, 2.1 MB) tracks 129 data points to determine how well the nation and individual states are prepared to handle widespread health emergencies. Not all data collected is directly medical; for example, the Index also looks at the condition of bridges.

The national score has climbed marginally in the past few years as some states work to improve their capabilities. Overall:

- Incident and Information Management scored highest at 8.7 out of 10.
- Healthcare Delivery scored lowest at 4.9.
- The number of states above the national average dropped to 11 in 2019 from 22 the previous year.
- 39 percent of the population reside in states with below-aerage health security.

Each state's data is available and provides a breakdown of the measures and the state's scores as well as where data is lacking. This information may help identify areas for improvement unique to each state and provides a defensible and persuasive data source to use when discussing policy changes and budget with state officials

(Source: NHSPI)

TRANSCAER seeking state and regional coordinators

TRANSCAER (Transportation Community Awareness and Emergency Response) is a voluntary national outreach effort focused on assisting communities to prepare for and to respond to a possible hazardous materials transportation incident. Created by Dow Chemicals and Union Pacific Railroad, TRANSCAER has been training first responders regionally to handle these incidents since 1986.

TRANSCAER is currently looking for volunteer State or Regional Coordinators for the following: District of Columbia; Hawaii; Iowa; Kansas; Maine; Massachusetts; Missouri; Montana; Oregon; Rhode Island; South Dakota; Vermont; Washington; Wyoming; and Region 4 (Alaska, California, Hawaii, Idaho, Montana, Nevada, Oregon, Utah, Washington, Wyoming).

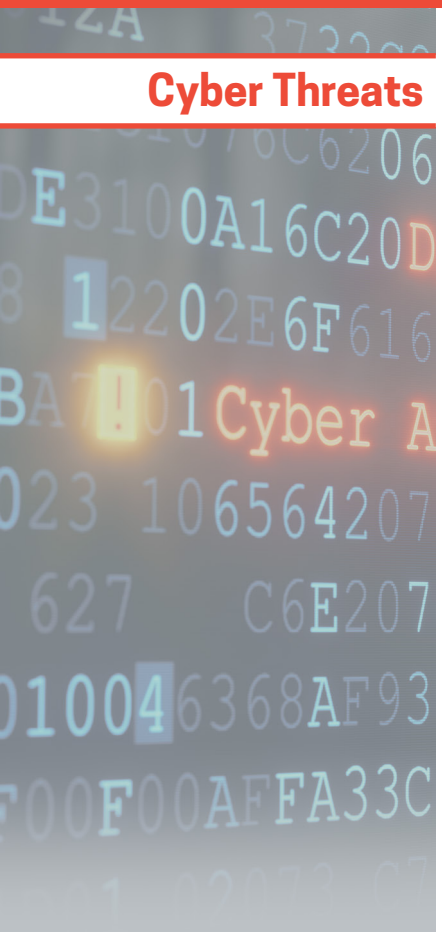
Responsibilities of a State/Regional Coordinator typically include:

- Establish a state/regional TRANSCAER Team comprised of chemical and transportation industry expertise, emergency responders and local emergency preparedness agencies. Recruit participation from safety/security agencies.
- Identify state TRANSCAER needs and opportunities.
- Provide speakers and/or make TRANSCAER presentations.
- Maintain a listing of state TRANSCAER activities, contacts, resources and speakers.
- Provide regular updates on state TRANSCAER issues.
- Commit 1-2 days a month to implementing TRANSCAER programs.

If you are interested in becoming a State or Regional TRANSCAER Coordinator please contact Director Erica Bernstein at ebernstein@chemtrec.com for an application.

(Source: TRANSCAER)

Cyber Threats



Webinar: Destroyer of Cities - Lessons from Ransomware Attacks

A rash of ransomware attacks has hit small and local governments in recent months. From a trio of municipalities in Florida, to the ongoing problems in Baltimore to the expensive remediation in Atlanta, city governments falling victim to ransomware has become all too common. This webinar will **look at 100 incidents from the last few years to highlight trends and lessons**.

(Source: MCPMag.com)

Cyber warfare threat rises as Iran and China form "united front"

Last week, the ICT ministers of Iran and China met in Beijing to discuss "common challenges" in the face of "US unilateralism." As a result of these developments, these two Untied States adversaries may eventually begin coordinating offensive cyber campaigns targeting US systems, which **could lead to further escalations in cyberspace**. The timing of the announcement is significant, since tensions between the US and Iran have escalated in recent weeks, while Washington is also engaged in fierce technological and trade competition with Beijing.

(Source: Forbes)

Florida jurisdictions beware: third city falls victim to ransomware

A third Florida local government has reported that it has been struck by ransomware. Key Biscayne joins Lake City as a victim of Ryuk, a form of ransomware first spotted in August of 2018. While the attack on Riviera Beach, Florida, was similar—**all three cases start with a city employee clicking on an attachment in email and unleashing malware**—it's not certain if that attack was also based on Ryuk.

(Source: ArsTechnica)

Before you hook up that printer to the IoT, read this

Seemingly every appliance we use comes in a version that can be connected to a computer network. But **each gizmo we add brings another risk to our security and privacy**. So before linking your office's new printer or coffee maker to the internet of things (IoT), have a look at an informational report from the National Institute of Standards and Technology (NIST) outlining these risks and some considerations for mitigating them.

(Source: zdnet)

Legacy Systems in the Healthcare Industry

Healthcare continues to increase the number of IoT and medical devices used in the healthcare setting, with the majority of devices operating on legacy systems. By 2020, **70 percent of all healthcare devices will be operating on Windows systems, which will no longer be supported by Microsoft** beginning January 14.

A lot of organizations aren't equipped to confront hardware hacking mainly because the technologies that they employ may continue to pose security vulnerabilities even at the end of their life cycles.

(Source: HC3)

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.