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

The InfoGram

Volume 19 — Issue 25 | July 18, 2019

Clark County Sheriff releases Route 91 shooting after-action report

Poor radio reception, numerous false reports of secondary shooters, general chaos created by the 22,000-strong crowd attempting to flee the scene, and responding to an active shooter who is in a position of advantage are some of the challenges mentioned in the "1 October After-Action Review" (AAR) (PDF, 6.25 MB) detailing response to the 2017 mass shooting.

This AAR is 164 pages and very comprehensive, detailing the mass casualty incident (MCI) timeline, the response timeline, training the department had already invested in, and more. There's far too much to summarize, but here are a few of the 93 recommendations:

- Provide additional training, including live exercises on MCI, for leadership at the rank of lieutenant and above, regardless of assignment.
- Maintain monthly meetings with key stakeholders in the tourism industry.
- Provide response training to hotel and casino industry stakeholders as well as community partners, schools, churches, and those supporting critical infrastructure.
- Supply officers with training and equipment to mark areas that have been cleared to prevent duplication of effort.
- Compile and release accurate, timely facts and maintain a running chronology of information released (e.g., a fact sheet).
- Explore the feasibility of establishing pre-identified locations, in proximity to officers working special events overtime, to store weapons and personal protective equipment for a quicker response in the event of an emergency.
- Establish an information technologies team that can respond and provide IT support during significant incidents and/or MCI.
- Create policy, procedures, and protocols to meet the mandates for releasing public records in large-scale incidents and/or MCI.

Because of the sheer size of tourism in Las Vegas, it is in a prime position to create a set of best practices and recommendations when it comes to incorporating the private sector, tourism stakeholders and venues in emergency planning. If your jurisdiction has tourism of any kind, be sure to go over the LVMPD AAR.

Please see the Federal Emergency Management Agency "1 October After-Action Report" on the Route 91 Harvest Festival for additional information and recommendations.

(Source: LVMPD)

Smoke alarms recalled due to risk of failure to alert

Last week, Universal Security Instruments announced a recall of about 180,000 10-year battery-operated ionization smoke and fire alarms sold in the United States. The manufacturer received 134 reports of failure to properly activate

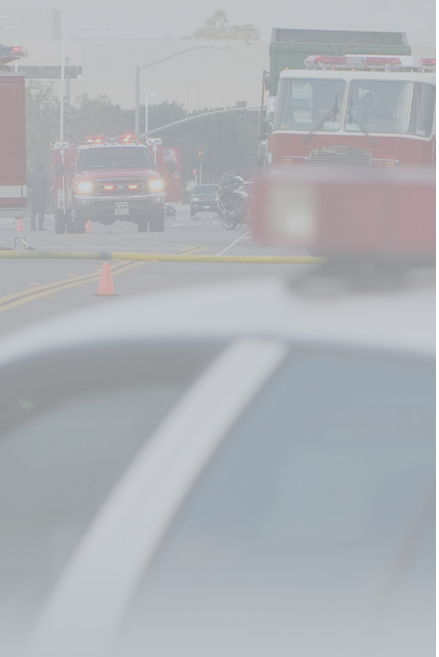
Highlights

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



during installation.

The Consumer Product Safety Commission (CPSC) and the Universal Security Instruments websites list model numbers of affected units and contact information.

Universal Security Instruments recommends consumers test these alarms and if alarm does not sound, consumers should contact Universal Security Instruments for a replacement.

Fire and public safety departments should share this information with their community through all means available.

(Source: CPSC)

CHEMTREC grant helps volunteer departments fund hazmat training

CHEMTREC has partnered with the National Volunteer Fire Council (NVFC) to award $7,500 to two volunteer fire departments in the United States. The awards are intended to help fire departments enhance their response capabilities and increase local preparedness to respond to and prepare for hazardous materials incidents.

Departments are eligible if they meet the following criteria:

- Must be all-volunteer or mostly volunteer (over 50 percent).
- Must serve a population of 25,000 or less.
- Be located in the United States and be legally organized under state law.
- Department/person applying on behalf of departments must be NVFC member.
- Demonstrate their need to receive the $7,500 award and in the application essay must describe the equipment, resources, and/or training the department would purchase and/or the training they would attend to increase their response capabilities for hazardous materials incidents. Please also describe the potential hazardous materials incidents that could occur in your community.

Only one application will be accepted per department. Any subsequent applications received for that department during the award year will be disqualified, so be sure to coordinate all efforts.

(Source: CHEMTREC)

NFPA Standard for An Active Shooter/Hostile Event podcasts

The Community Oriented Policing Services (COPS) Office's Active Shooter Podcast Series has two available podcasts focusing on the National Fire Protection Association (NFPA) 3000 Standard for An Active Shooter/Hostile Event Response Program.

The first is an overview of NFPA 3000 and why it is relevant for law enforcement agencies as well as fire departments. The presenter discusses why NFPA 3000 does not recommend tactics but instead lists benchmarks to hit within your jurisdiction or department based on your specific needs and capabilities.

The second focuses on planning for victims of mass shootings. The presenter from the Department of Justice's Office for Victim of Crime explains why it's important for victim services personnel to be included in your planning, training and exercise programs.

These podcasts and their transcripts are available for viewing or download.

(Source: COPS)

Cyber Threats

Coast Guard issues cybersecurity warnings for commercial vessels

The United States Coast Guard issued a safety alert advising commercial vessel owners and operators to ensure effective cybersecurity measures are in place to protect the network and important control systems on their ships.

The alert points to a February 2019 incident where **a vessel bound for the Port of New York and New Jersey had its systems infected with a piece of malware** that "significantly degraded the functionality of the onboard computer system."

The incident highlighted the lack of proper cybersecurity measures. Port authorities should be aware of the security ramifications of this issue.

(Source: Security Week)

Deepfake videos: nearly impossible to know the video isn't real

Deepfakes are a new breed of fake videos that use artificial intelligence (AI) to make a falsified video virtually undetectable by swapping out someone's face and voice with an imposter's. The consensus among researchers is that **deepfakes will eventually be used to impact a political election** in the near future. This is much more than a Photoshopped meme or a fake news story. It's nearly impossible to know that the video isn't real.

(Source: TechRepublic)

Webinar: IoT Applications and Instant Networks for Law Enforcement

The Internet of Things (IoT) opens the doors for rapidly deployable temporary networks. A temporary pop-up network, such as an Emergency Command Center or even a command vehicle at a large event, helps public safety officials monitor large gatherings of people to ensure maximum community safety.

These pop-up networks also aid in disaster recovery from events such as hurricanes, earthquakes, wildfires and human-caused events like terrorist attacks and active shooters.

Join the Justice Clearinghouse on Tuesday, July 30, 2019, from 1-2 p.m., for a webinar discussing these technologies. Registration is required. The information in this webinar will benefit all first responder fields.

(Source: Justice Clearinghouse)

Mayor group adopts resolution not to pay any more ransoms to hackers

The US Conference of Mayors unanimously adopted yesterday a resolution not to pay any more ransom demands to hackers following ransomware infections. The resolution adopted this week at the 87th annual meeting of the US Conference of Mayors doesn't have any legal binding, but can be used as an official position to justify administrative actions, for both federal authorities and taxpayers alike.

Hackers exploit the fact that some cities fail in backing up their data and are left with no choice but paying to recover crucial documents or face huge fines.

Both the FBI and cyber-security experts usually advise against paying the ransom demand, unless there's no other way to recover data. Everyone is urging municipalities to set up basic data back-up routines.

(Source: zdnet)

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.