EMR-ISAC
Emergency Management & Response-Information Sharing & Analysis Center

The InfoGram

Volume 16 – Issue 29 *July 21, 2016*

Highlights:

The U.S. Fire Administration maintains 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.**

Los Angeles Studies Paris Attacks

In April, Los Angeles sent a multi-agency delegation to Paris to meet with their French counterparts in law enforcement, intelligence, and public safety to learn about the November 2015 attacks. They identified best practices and lessons learned, bringing those findings home to apply to plans and training, publising them in a White Paper.

"The Attacks on Paris - Lessons Learned: a Presentation of Findings" looks at six areas: intelligence, community engagement, investigation, incident command, crisis communication, and training/equipment. The paper provides a summary of the attacks in Paris, discusses prior attacks in France, and other high-profile attacks in Europe.

Any community looking to bolster its planning, response, and recovery efforts for such an attack should consider reading this concise 32-page White Paper. The lessons learned talk about differences in the way the two countries manage these incidents, point out weaknesses in the current systems that can easily be addressed, and what authorities learned and changed from prior attacks.

(Source: HSDL)

Cybersecurity Guide for Law Enforcement Agencies

The National Consortium for Advanced Policing released "Cybersecurity Guide for State and Local Law Enforcement" (PDF, 1.3 Mb), a much-needed addition to the body of information available to law enforcement on cybercrimes. The guide is intended to help state and local law enforcement agencies protect themselves from cybercrimes while also responding to cyber threats reported in the community.

Cybersecurity takes on more significance for law enforcement due to the nature of the work. In addition to malware and viruses, unsecure information within networks can lead to case information being stolen or even altered. The guide discusses successful attacks against law enforcement agencies and the types of threats they face.

Also available is an issue brief on the same topic, "A Policy Roadmap to Enhance Capabilities" (PDF, 736 Kb), which focuses on what policymakers can do to improve the cyber authority and capabilities of state and local law enforcement.

These documents makes this murky subject more accessible to law enforcement agencies, and prioritizes the steps agencies can take toward cybersecurity.

(Source: Law Enforcement Cyber Center)

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.

Popular Game a Problem for Authorities, Business

By now, you've very likely seen or heard stories about the downsides of the popular new augmented-reality game Pokemon Go. There are reports of assaults, robberies, injuries, and even stabbings and sexual assaults in the short time since the game's release. One young woman even found a dead body.

These all increase emergency calls, but first responders have other things to watch for with this game. As players hunt for virtual Pokemon, they will be drawn into areas that their cellphone maps tell them to go, which may lead them into restricted areas on public or private property. This includes reports of trespassers at fire stations, military bases, critical infrastructure sites, and detention and rehabilitation centers. In addition to trespass calls, this can increase the potential for surveillance and suspicious activity reporting.

Employers are also trying to manage both employees playing on company time and the cyber threat that comes with increased presence and use of personal devices. The game requires so much access to your phone's features that, should a hacker gain access with malware, they would get ahold of a great deal of personal or business information. In addition, because so many people are using Google accounts to log in, hackers may be able to exploit a flaw allowing access to Google accounts without permission. Workplaces may want to review "Bring Your Own Device" policies.

If your public or private sector location is currently an unwilling piece of the Pokemon Go universe, you can attempt to "opt-out" using this form on the developer's website. Players can also opt-out of allowing the game to have so much access to their data.

(Source: Forbes)

Radiological/Nuclear Training for HazMat Techs

The Counterterrorism Operations Support (CTOS) Center for Radiological/Nuclear Training is hosting several residential training courses available for HazMat technicians. "Weapons of Mass Destruction Radiological/Nuclear Course for Hazardous Material Technicians" (PDF, 93 Kb) has several openings through fall 2016, and more courses are scheduled through July 2017.

The exercise-based course trains emergency responders to manage radiological weapons of mass destruction incidents while mitigating health risks. It covers applied radiation theory, health effects, and terrorist use of radiation and radiological materials. Participants will use detection equipment and survey techniques, and will go through drills and exercises using radioactive materials.

This is a 4-day residential course at the Nevada National Security Site. It is a federally-funded training free to qualified state, local, territorial, and tribal responders. Covered expenses include flight, mileage, parking, hotel, per diem, and tuition. Travel days are Sunday and Friday. It is not required but is recommended that participants be Certified Hazardous Materials Technicians.

First responders are also eligible to retake this training three years from the last completion date. CTOS has made significant improvements in course curriculum and to the training venues over the last few years. If you have taken the course more than three years ago you are invited to retake it. Please see the online schedule for class dates and registration information.

(Source: CTOS)

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local *FBI office* and also the *State or Major Urban Area Fusion Center*.

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at **202-282-9201**, or by email at **nicc@dhs.gov**.