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

The InfoGram

Volume 18 — Issue 47 | November 29, 2018

After-action review of fire response to Pulse nightclub shooting

The National Police Foundation (NPF) conducted an objective and in-depth review of the Orlando Fire Department's (OFD) response to the 2016 Pulse nightclub shooting, at the request of the City of Orlando and the OFD. The report provides direction and recommendations beneficial to all fire/EMS providers nationwide.

The NPF review focuses on leadership, interagency relationships, command and tactics, training, equipment, policies and SOPs, communications and post-event responder wellness. Many interviews were conducted, and the review team created a comprehensive timeline and maps to better understand the incident response. Some of the findings:

- Mutual aid agreements worked and ensured needed personnel and equipment arrived quickly.
- Due to a combination of circumstances, OFD executive leadership did not know of the incident until approximately three hours after it began.
- There was no unified command and poor inter-agency communication.
- Employees at all levels were either unaware of policies and procedures or actively chose not to follow them as they believed them to be outdated.
- Policies and procedures were not consistent with training.
- The level of trauma first responders experienced was not fully appreciated, recognized or addressed.

Since Pulse, OFD has implemented a variety of improvements addressing some of the items listed above and is actively working on updating policies and procedures. Other fire departments are urged to read this review and consider their own policies and procedures, training program and mutual aid agreements, and to hold exercises with their local law enforcement.

(Source: NPF)

DHS Regional Resiliency Assessment Program

The Regional Resiliency Assessment Program (RRAP) is a voluntary program to assess specific critical infrastructure jointly with local agencies and authorities. It analyzes security and resilience gaps, guides risk management decisions, and can improve partnerships between the public and private sectors.

Projects are generally at least a year and include data collection and analysis along with continued technical assistance to enhance the infrastructure's resilience. Data exchange opportunities often include first responder capability assessments, voluntary facility and security surveys, and targeted studies.

Examples of RRAP projects:

- Physical internet infrastructure vulnerabilities in Loudon County, Virginia. The area serves as the primary global internet traffic hub on the east coast.

Highlights

U.S. Fire Administration

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

- New York City's healthcare supply chain.
- Transportation infrastructure in the Western Washington earthquake zone (PDF 226 KB), coincided with the Cascadia Rising exercise.
- Identifying biosecurity hazards and gaps in the Texas panhandle's beef industry.

RRAP projects are selected each year by the Department of Homeland Security (DHS) with guidance from federal, state and local partners. Those interested in projects can email Resilience@hq.dhs.gov for more information.

(Source: DHS)

New Cybersecurity and Infrastructure Security Agency

Earlier this month, the president signed legislation creating the Cybersecurity and Infrastructure Security Agency (CISA), giving the Department of Homeland Security the lead in national efforts to secure the nation's critical infrastructure from physical and cyber threats.

The creation of CISA elevates the mission of the former National Protection and Programs Directorate within DHS. CISA will be divided into three divisions:

- Cybersecurity - will lead efforts to protect the federal .gov domain and collaborate with the private sector .com domain to increase critical network security.
- Infrastructure Security - conducts assessments to help critical infrastructure owner, operators, and state and local governments understand their risks.
- Emergency Communications - leads the nation's operable and interoperable national security and emergency preparedness communications. This includes providing outreach, training, tools and guidance to all levels of government.

(Source: CISA)

Webinar: A Culture of Preparedness

On December 6, 2018, from 1-2 p.m. Eastern, the National Information Sharing Consortium is hosting the webinar "A Culture of Preparedness: Federal, State, and Local Training Resources" with the District of Columbia Homeland Security and Emergency Management Agency (DC HSEMA).

During this webinar, DC HSEMA will discuss how the District of Columbia assesses its emergency management training gaps. It will show benefits for organizations to make training decisions based on information derived from the assessments, strategies and plans developed during the Preparedness Cycle.

DC HSEMA will also provide an overview of training resources available for first responders, homeland security officials, emergency management officials, private and non-governmental partners throughout the nation.

(Source: NISC)

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.**

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.