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

INFOGRAM 40-11 October 6, 2011

NOTE: *This INFOGRAM will be distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures. For further information, contact the Emergency Management and Response- Information Sharing and Analysis Center (EMR-ISAC) at (301) 447-1325 or by e-mail at emr-isac@dhs.gov.*

Residential Building Fires Topical Report
(Source: U.S. Fire Administration)

The U.S. Fire Administration (USFA) announced last week the release of a special report focusing on the causes and characteristics of fires in residential buildings. The report, "Residential Building Fires," (PDF, 973 Kb) is part of the Topical Fire Report Series and is based on 2007 through 2009 National Fire Incident Reporting System (NFIRS) data.

According to the USFA Press Release, residential buildings are one- or two-family dwellings or multifamily structures. The term also includes manufactured housing, hotels and motels, residential hotels, dormitories, assisted-living facilities, and halfway houses.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) observed in the report that an estimated 374,900 residential building fires are reported to U.S. fire departments each year and cause an estimated 2,630 deaths, 13,075 injuries, and $7.6 billion in property loss. Cooking is the leading cause (44 percent) of residential building fires.

Assessing Vulnerability in Communities
(Source: U.S. Fire Administration)

Last week, the U.S. Fire Administration (USFA) issued a "Coffee Break Training" (PDF, 372 Kb) pertaining to "Assessing Vulnerability in Your Community." The objective of the USFA paper is to explain the concept of vulnerability and its relationship to overall community risk from a firefighting perspective. It affirms that each hazard must be viewed from the community's vulnerability.

The training brief explains that vulnerability is the susceptibility to suffer harm or loss from an event. It conveys that vulnerability may vary based on numerous factors such as preparedness, capability of emergency services, etc. "Vulnerability may also vary for the same hazard from area to area in the same community."

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) noted in the paper the elaboration of five areas of vulnerability in a community: human, economic, social, political, and environmental. According to the FEMA Fact Sheet (PDF, 190 Kb) titled "State and Local Mitigation Planning," hazard mitigation planning is the process used to identify these vulnerabilities and to develop long-term strategies for protecting people and property in future hazard events. History demonstrates the losses caused by these vulnerabilities can be significantly reduced through comprehensive multi-hazard mitigation planning.

National Cybersecurity Awareness Month
(Source: DHS)

On 3 October 2011, President Obama issued a presidential proclamation announcing the eighth annual National Cyber Security Awareness Month. This year's theme emphasizes that everyone has shared responsibility in protecting against cyber threats and cyber crime.

For all its advantages, increased interconnectivity also brings heightened risk of theft, fraud, and abuse to individuals, businesses, communities, governments, and even the nation's emergency services. National Cyber Security Awareness Month is an opportunity to engage public and private sector stakeholders, as well as the general public, to create a safe, secure, and resilient cyber environment.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) recognizes that this month also marks the first anniversary of the Stop.Think.Connect™ Campaign, which is the national public awareness effort to guide the nation to a higher level of Internet safety.

Throughout the month of October and beyond, personnel of Emergency Services Sector departments and agencies are urged to practice safe online habits, particularly in the workplace. The following simple steps can help keep organizational and professional information safe online:

- Set strong passwords, and don't share them with anyone.
- Restrict access to personal information of employees and citizens to prevent identity theft.
- Be suspicious of unsolicited contact from individuals seeking internal organizational data or personal information.
- Immediately report any suspicious data or security breaches to your supervisor and/or authorities.

To learn more about National Cyber Security Awareness Month and the *Stop.Think.Connect™* Campaign, including additional tips and resources to stay safe online, visit Cybersecurity or the Campaign website.

Private Sector Resources Catalog 3.0

(Source: DHS)

Recently released as the second update to the original, the Private Sector Resources Catalog 3.0 (PDF, 1.1 Mb) was developed to facilitate private sector access to all Department of Homeland Security (DHS) resources. The document, which contains a comprehensive listing of DHS resources, aims to help private sector organizations deal with a plethora of homeland security issues.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) determined that the 64-page catalog has over 400 entries covering tornado safety to critical infrastructure protection. It has been reorganized by categories, such as cybersecurity, immigration law, and preventing terrorist activities.

Divided into 17 categories, the terrorism prevention section discusses topics such as bomb prevention, mass transit, land transportation, facility security, hazardous materials, and maritime security, among others. It further contains an index listing resources by type including, brochures, reports, exercises, training, and more, much of which may have information value to Emergency Services Sector departments and agencies.

REPORTING NOTICE

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. FBI phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm. Fusion Center information can be seen at http://www.dhs.gov/contact-fusion-centers.

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.

When available, each report submitted should include the date, time, location, type of activity, number of people, equipment used for the activity, name of submitting person and organization, and a designated point of contact.