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

INFOGRAM 28-11 July 14, 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.*

Managing the Wildland-Urban Interface
(Source: FireRescue1)

The wildland-urban interface (WUI) firestorms in several states this year demonstrate that they are among the most dynamic, dangerous, destructive, and costly fires in the world, according to an article in FireRescue1.com. For deployed firefighters, "the wildfires have a minefield of risk with extreme fire behavior, eclectic fuel loading, unrealistic public expectation, high media interest, and a fluid mix of multi-agency responders of varying abilities."

It is widely recognized that the high resource impact, diverse challenges, and imposing risks of WUI events require disciplined management and a meticulously planned and executed response. The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) observed in the cited article that the author offers the following six factors for deliberate consideration when formulating the "strategies and tactics" to manage WUI conflagrations:

- Number, type, and experience level of response personnel and apparatus.
- Evacuations, traffic, and other public considerations.
- Fuel type, weather conditions, and terrain features.
- Size and availability of safety zones.
- Number of structures, construction type, defensible space, power lines, vegetation, vehicle access, and water supply.
- Current and expected fire behavior, and how much preparation time.

The National Cohesive Wildland Fire Management Strategy (PDF, 1.7 Mb) indicates that addressing wildfire is not simply about fire management, fire operations, or WUI problem. It is a larger, more complex land management and societal issue. The following websites provide more information for the comprehensive undertaking of managing WUI blazes:

- Incident Response Pocket Guide (PDF, 930 Kb)
- Wildland-Urban Interface Tips
- Wildland-Urban Interface Links

Amateur Radio Community
(Source: American Radio Relay League)

Considering the requirement for emergency communications during a major disaster, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) examined the variety of roles performed by amateur radio operations. In a 3 May forum on earthquake communications preparedness, discussed in a news release by the American Radio Relay League (ARRL), Federal Emergency Management Agency Administrator Craig Fugate described the amateur radio operator as "the ultimate backup." He explained that amateur radio volunteers use their own time and resources to help get the word out in the critical first hours of a disaster.

There are two groups of volunteer radio operators that provide assistance during an emergency: Radio Amateur Civil Emergency Service (RACES) and Amateur Radio Emergency Service (ARES). RACES operators, who are registered with state and local governments, are activated after an emergency declaration. They usually operate from state emergency operations centers. ARES members provide emergency communications before an emergency has been officially declared. Many radio operators participate in both organizations.

During the communications forum, Administrator Fugate explained that there is a tendency to dismiss the crucial role of amateur radio operations. To ensure essential communications when disaster occurs, particularly when wired and wireless systems fail, he recommended the inclusion of the amateur radio community in emergency communications plans. He stated: "Amateur radio oftentimes is our last line of defense."

See the WJHG article for a recent example of how amateur radio operators have become capability multipliers during local emergencies.

Cyber Terrorism Awareness

(Source: ComputerWeekly.com)

Although there is currently no evidence of systematic cyber terrorism, ComputerWeekly.com reported in a 12 July article that cyber terrorism will become an increasing problem as the tools and techniques needed for cyber attacks become more widely available. Based on her research, the author wrote: "Terrorists are utilizing a range of new technologies to ramp up attacks."

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) learned that nationwide electronic data networks are intimately linked to practically all elements of daily life, including critical infrastructures such as the emergency services, which includes 9-1-1 centers. This reliance on networked operations and wireless data systems increases the potential for the exploitation of gaps in electronic defenses.

The U.S. Computer Emergency Readiness Team (US-CERT) prepared numerous cyber security tips to mitigate or eliminate the threat of a cyber attack by domestic criminals or transnational terrorists. The following salient recommendations have been summarized for the benefit of emergency departments and agencies:

- Ensure that all computers have updated security software (i.e., anti-spyware, anti-virus, and firewall), Web browsers, and operating systems.
- Set policy requiring employees to use long, complex passwords that they change at least every 60 days.
- Include or update cybersecurity practices in employee handbooks and insert policies regarding the use of mobile devices and laptops when offsite.
- Create a recovery or restoration plan in case of data loss.
- Initiate policy to turn computers off at night and other down times.
- Delete unused and old data.
- Remain current on trends in cybersecurity and emerging threats.

Additional information to protect against cyber terrorism can be seen at staysafeoneline.org and at onguardonline.gov.

Continuity of Operations Webinar Series

(Source: FEMA)

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) was notified about the start of the monthly continuity of operations webinar series offered by the Federal Emergency Management Agency (FEMA). The webinars are specifically designed for those who plan, train, and manage continuity of operations programs.

The webinars occur the first Wednesday of every month at approximately 2 p.m. EST. Each 45-minute webinar includes a 10-minute Question and Answer session. FEMA indicated that the webinars are an opportunity to meet with continuity experts across the emergency management family and share best practices on how government, organizations, and communities can prepare for and recover from a disaster.

More information can be obtained at the designated webinar website. To request additional information or to register for the webinars, send an email to FEMA-ContinuityWebinar@dhs.gov.

DISCLAIMER OF ENDORSEMENT

The EMR-ISAC does not endorse the organizations sponsoring linked websites, and does not endorse the views they express or the products/services they offer.

FAIR USE NOTICE

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.