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

INFOGRAM 39-07 October 4, 2007

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.*

Cyber Security

In his opening remarks this week at the kick-off summit of the 4th annual Cyber Security Awareness Month, Department of Homeland Security (DHS) Assistant Secretary for Cyber Security and Communications Greg Garcia said, “Our mission is clear. Securing the systems that maintain and operate critical infrastructures is vital to national security, public safety, and economic prosperity.”

The Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC) confirms that computers and cyber networks are an integral part of the critical infrastructures of the Emergency Services Sector (ESS) that cannot be interrupted or destroyed. Moreover, unprecedented interdependencies continue to create vulnerabilities with potential disruptions to ESS services such as computer aided dispatching.

Assistant Secretary Garcia explained, “We all depend on shared critical infrastructures and systems to maintain our national security.” He called on every person who uses networked technology to take personal responsibility for securing their part of cyberspace by taking cyber risks seriously, ensuring that any potential cyber incidents, threats, or attacks are reported to the U.S. Computer Emergency Readiness Team (US-CERT) at (888) 282-0870, and by using the safeguards available at the federal web site OnGuardOnline (http://onguardonline.gov/index.html).

Among the resources available at the web site are brief tests to measure computer users’ abilities to detect and avoid unwanted (spam) electronic messages, and social engineering attacks such as phishing. The site also offers current advice on laptop computer security, an important topic as their use by responder organizations increases. Additional information about workplace computer security issues and protection strategies can be reviewed in the brief article, “Are You Your IT Department’s Worst Nightmare?” at http://www.govtech.com/gt/print_article.php?id=150205.

Hybrid Gangs

Gang violence is among the growing threats to the safety and operations of Emergency Services Sector (ESS) departments and agencies, in addition to the protection of community critical infrastructures. The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) recently learned from media accounts that gangs referred to as “hybrids” are beginning to arrive in cities throughout the Nation, most frequently in communities that have not experienced the gang problems which have plagued some cities since the 1980s.

Hybrids bear little resemblance to traditional gangs, such as MS-13 (Mara Salvatrucha), described in past INFOGRAMs, yet ESS officials point to hybrids as one of the reasons for fresh surges in gang violence. In some jurisdictions, 40% to 50% of gangs are now hybrids.

There are a number of significant differences between traditional and hybrid gangs. One is that hybrid members are unlikely to wear gang "colors" or gang-specific paraphernalia, making them harder to identify. Hybrids tend to be comprised of members of different racial/ethnic groups who participate in a single gang or in multiple gangs. There are additional differences: former rivals often cooperate, hybrid members are typically younger than traditional gang members, and the rules or codes of conduct are unclear. The primary goal of hybrid gangs, experts say, is to make money through illegal activities.

Law enforcement personnel describe hybrid gang members as "trigger-happy," with a tendency to use their weapons simply to use them, in some cases, shooting at other gangs from opposite sides of streets and, in one instance, in a gated community. Their open and aggressive willingness to inflict bloodshed threatens responders and the communities they serve.

The EMR-ISAC encourages emergency personnel to be alert to the emergence of hybrid gangs in their municipalities, and review appropriate safety and force protection techniques for response to gang-related activities. The EMR-ISAC further encourages ESS organizations to consult gang deterrence specialists or a Regional Area Gang Enforcement Unit if they suspect the presence of hybrid gangs in their jurisdiction.

Military Guide to Terrorism

American counterterrorism officials continue to caution the Emergency Services Sector (ESS) about the growing threat of incidents that could potentially occur on domestic soil. Considering recent arrests in New York, Georgia, California, Connecticut, and New Jersey, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) understands that the threat to National critical infrastructures from domestic terrorism is real.

The newly updated *Military Guide to Terrorism in the Twenty-First Century* is a source of information to help ESS personnel protect themselves, their organizations, and their response-ability.
The guide is a high-level terrorism primer that addresses foreign and domestic threats against the U.S. in a contemporary operational environment. Prepared by the Intelligence Support Activity of the U.S. Army Training and Doctrine Command, and approved for public release, it includes an overview of the history of terrorism, descriptions of terrorist behaviors and motivations, a review of terrorist group organizations, and the threat posed to the United States and overseas. It also provides information on various terrorist groups, the terrorist planning cycle, operations and tactics, firearms used by terrorists, Improvised Explosive Devices, conventional munitions used by terrorists, and a discussion on Weapons of Mass Destruction.

To view and download *A Military Guide to Terrorism in the Twenty-First Century*, visit http://www.fas.org/irp/threat/terrorism/index.html.

Injury Risk to EMS Providers

A steady increase in obesity rates in the United States "poses a threat to emergency services," according to reports examined by the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC). The climbing obesity rates are affecting the personnel and physical infrastructures of the Emergency Services Sector (ESS).

Recent studies by the American College of Emergency Physicians and the National Association of EMTs found that nearly half of providers had suffered back injuries, most often as a result of lifting extremely heavy patients. A prominent Emergency Medical Services (EMS) director said that, "Extricating these patients from crashes takes longer, is more difficult, and moving them from their homes to the ambulance, down three flights of stairs, is dangerous to providers." Also, because additional crews often must be called to assist, EMS administrators "must plan for two or three EMS units to be out of the system for a few hours on one such assignment," according to JEMS.com.

Few ESS departments presently have the special stretchers and patient-moving devices to handle weights that exceed 350 pounds. Larger ambulances may be necessary to safely transport heavy patients while at the same time maintaining their dignity. Departments that have purchased the larger vehicles have found their cost to be approximately $125,000 each versus about $75,000 for a regular ambulance.

The recent JEMS.com article, “Bariatric Patients Pose Weighty Challenges,” offers guidance for EMS agencies to address the medical and operational challenges posed by large patients, while also acknowledging the sector’s fiscal realities. It encourages emergency medical organizations to conduct periodic training on both emergency and non-emergency transports and include fire and law enforcement departments if they are used to augment EMS staff in the community. Among the suggestions is that the EMS consider creating a special response unit that could be shared as a regional resource.

The full article is available at http://www.jems.com/news_and_articles/articles/Bariatric_Patients_Pose_Weighty_Challenges.html.

FAIR USE NOTICE

The National Infrastructure Coordinating Center (NICC) within the Department of Homeland Security (DHS) Office of Infrastructure Protection is the central point for notifications regarding infrastructure threats, disruptions, intrusions, and suspicious activities. Emergency Services Sector personnel are requested to report any incidents or attacks involving their infrastructures using at least the first and second points of contact seen below:

1) NICC - Voice: 202-282-9201, Fax: 703-487-3570, E-Mail: *nicc@dhs.gov*
2) Your local FBI office - Web: *http://www.fbi.gov/contact/fo/fo.htm*
3) EMR-ISAC - Voice: 301-447-1325, E-Mail: *emr-isac@dhs.gov*, fax: 301-447- 1034,
Web: *www.usfa.dhs.gov/subjects/emr-isac*, Mail: J-247, 16825 South Seton Avenue,
Emmitsburg, MD 21727