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

INFOGRAM 22-07 June 7, 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.

Complacency and Mediocrity

For nearly six years the United States has enjoyed the absence of a major terrorist attack. Much credit for this belongs to the many public and private organizations that altered their plans, training, and operations to prevent and protect against the next man-made catastrophe. Despite severely restrained resources, these departments and agencies avoided complacency and mediocrity by improving their capabilities to deter or mitigate the cataclysmic effects from all hazards.

Nevertheless, recent reports from around the nation cite continuing preparedness gaps for both man-made and natural disasters at the local, regional, and tribal levels. Some security specialists speculate that a "false sense of security," growing weariness, and complacency have caused the lack of progress at the thousands of American localities not affected by a major calamity. In response, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) suggests that any gaps in infrastructure protection are potentially dangerous and undesirable, particularly among ranks of Emergency Services Sector (ESS) personnel.

The EMR-ISAC recognizes the ongoing terrorist planning as exemplified by the plots against Fort Dix (NJ) and JFK Airport (NY), as well as the prospects for a natural disaster anywhere in the country. Therefore, this ISAC encourages ESS organizations to prolong their efforts against complacency and mediocrity by considering the following reflective questions. Answers to these questions will help assess the degree of basic readiness and response-ability for all-hazard incidents:

- Are leaders more knowledgeable and capable to manage massive emergencies in their jurisdiction?
- Have personnel been thoroughly trained to survive and successfully perform in all hazards?
- Have measures been implemented to ensure all personnel are informed when an event occurs?
- Have there been deliberate actions to identify and protect internal critical infrastructures?
- Have emergency plans been revised, distributed, and rehearsed for all probable contingencies?
- Have leaders arranged for regional response options to maximize capabilities?
- Have approved plans been fully coordinated and rehearsed with automatic and mutual aid partners?
- Do provisions exist to guarantee the continued supply of food, fuel, etc., for extended operations?
- Have the National Incident Management System and Incident Command System been effectively incorporated into plans, training, and operations?
- Is the organization receiving the EMR-ISAC CIP (FOUO) Notices about threats and vulnerabilities, which could make a difference in emergency plans and operations during elevated threat levels? (If not, write to the EMR-ISAC at emr-isac@dhs.gov.)

MS-13 Domestic Gang Violence

Although much attention is given to transnational terrorism, law enforcement sources substantiate that gang violence is a growing threat to the safety and operations of Emergency Services Sector (ESS) departments and agencies in addition to community critical infrastructures. For example, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) points to the brutal MS-13 street gang that continues to spread throughout the nation. This gang, also known as "Mara Salvatrucha," consists largely of illegal aliens from El Salvador and other Latin American countries.

MS-13 is an opportunistic criminal group whose members migrate throughout the United States and abroad. It recruits new members by glorifying the gang lifestyle and absorbing smaller gangs. Middle and high school students are frequently targeted for recruitment.

Mara Salvatrucha engages in a wide range of criminal activities, including homicide, rape, sexual assault, robbery, battery, burglary, home invasion, vandalism, car hijacking, drug distribution, prostitution, immigration offenses, and weapons violations. Gang members use violence or threats of violence to intimidate police officers, resist arrest, and to interfere with criminal investigations.

Since MS-13 members have directed death threats toward law enforcement officers, the EMR-ISAC recommends extreme caution by emergency personnel when performing duties with suspected gang participants or working in areas where gang members typically congregate. Appropriate safety and force protection techniques must be used when responding to disorderly groups, loud parties, etc., to avoid being ambushed by other hiding gang members. This group has a notorious reputation for employing deception and surveillance activities to collect information for ruses to entrap their victims.

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 MS-13 in their jurisdiction.

Mail Bomb Threats

Most chief officers of Emergency Services Sector (ESS) departments and agencies would probably consider the risk of receiving a bomb in the mail to be somewhat minimal. However, these same community leaders would not assume it could never happen. Yet, government security experts state that mail handling in public and private sector emergency organizations is "the most overlooked area when applying security policies and procedures."

Counterterrorism specialists maintain that organizations must have a comprehensive bomb threat response plan in place, which all assigned personnel regularly rehearse. When properly planned, implemented, and tested, the plan will prevent an actual bomb threat from creating the chaos within an ESS unit that could temporarily disrupt operations and degrade response-ability.

To prevent the adverse effects of a letter or parcel bomb threat among emergency departments and agencies, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) summarizes the following typical suspicious characteristics from a mail security article seen in the May issue of the *Homeland Defense Journal*:

- Arrives unexpectedly from an unfamiliar source.
- Addressed to someone no longer in the organization.
- Marked with restrictive endorsements such as "personal" or "confidential."
- Has excessive postage, poorly typed address, incorrect titles, misspellings, etc.
- Weighs unusually more for the size of the envelope or package.
- Has no return address or an invalid return address.
- Has a powdery substance on the outside.
- Has an uncommon size or shape.
- Has an excessive amount of tape.
- Has a strange odor or stains.

Continuity of Communication Operations

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) reviewed current hurricane planning sources that discussed successful continuity of communication operations based on the Hurricane Katrina experiences of a number of Gulf Coast organizations.

Forecasters predict the 2007 Atlantic hurricane season that began on 1 June will be "very active." The EMR-ISAC, aware of the potential for this season's storms to seriously challenge the "response-ability" of the Emergency Services Sector (ESS), offers the following communications-related suggestions sector leaders can consider while preparing for a hurricane or any other hazard:

- Collect and maintain up-to-date contact information for employees, key vendors, suppliers, and service companies. Collect primary and secondary contact information and ensure that more than one channel is available to reach each person.
- Perform periodic, unannounced personnel accountability checks that ensure two-way communication with employees.
- Ask vendors and suppliers to explain their business continuity and disaster recovery plans, including methods of communicating with them in case of a crisis.
- Conduct a "no warning" test of the emergency plan. Practice executing it by occasionally having at least several key officers or leaders "out of the loop" to ensure that their deputies and assistants are able to administer the plan, send out notifications, perform roll calls, and conduct emergency operations.
- Verify that key staff can be reached via one or more avenues: cell phones, pagers, home phones, remote office phones, radios, etc. Determine how mission-essential action items can be escalated if key members cannot be contacted within a prescribed amount of time.
- Consider options for alternate meeting locations in hurricane- or tornado-prone areas, and publicize the chosen location and an alternate to all personnel. If all forms of communication were to fail, a personnel roll call could be conducted at a check-in location or assembly point.
- If employees use an alternate e-mail system (e.g., their personal e-mail accounts) to conduct business during or following a storm, require that all communications are archived to ensure a continuous electronic information trail.

According to multiple sources, organizations that fared well after Hurricane Katrina were not necessarily the largest or best funded. However, their emergency plans were well-thought-out, practiced, and, above all, emphasized communications with employees during a crisis. The EMR-ISAC encourages ESS leaders to plan and practice disaster communications strategies to enhance continuity of operations for all man-made and natural disasters.

To acquire a subscription to this weekly CIP INFOGRAM provided by the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC), follow the explicit instructions at: https://disasterhelp.gov/suite/doc/32357.

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