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

INFOGRAM 10-08 March 13, 2008

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.

ESS Suspicious Activity Reporting

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) acknowledges that the use of non-law enforcement Emergency Services Sector (ESS) personnel as antiterrorism sensors is controversial and potentially problematic, despite being advocated by academic papers, professional journals, and best-practices documents. Nevertheless, the EMR-ISAC continues to find instances where firefighters, emergency medical technicians, and paramedics—in the performance of normal duties—have appropriately assisted antiterrorism measures.

For example, local firefighters in Indiana recently saw a man approach a church, drop a backpack near the front door, and hurriedly walk away from it. Believing the action was suspicious, the firefighters kept the individual in sight until arrival of the police. The backpack was soon secured and detonated by the sheriff's department. Upon questioning by law enforcers, "the subject acted strangely and did not make any sense when he spoke," reported the police chief. Although he remains a "person of interest," the man was later released without being charged with a crime.

Agreeing that there are legally acceptable ways for first responders who are not sworn officers of the law to support community antiterrorism and critical infrastructure protection efforts by suspicious activity reporting, the EMR-ISAC offers the following list of questionable activities compiled by the FBI and seen at FBI.gov:

- Surveillance—Anyone monitoring or video recording activities, taking notes, using cameras, maps or binoculars near key facilities or major events.
- Suspicious Questioning—Anyone attempting to gain information in person, by phone, mail, or e-mail about a key facility or the people who work there.
- Tests of Security—Anyone attempting to penetrate or test physical security or procedures at a key facility or major event.
- Acquiring Supplies—Anyone trying to acquire explosives, weapons, ammunition, dangerous chemicals, flight manuals, uniforms, or identification for key facilities or major events.
- Suspicious Persons—Anyone who does not appear to belong in the workplace or business establishment or near a key facility or event.
- Practice Runs—Any behavior that appears to be preparation for a terrorist act, such as mapping out routes, playing out scenarios, monitoring key facilities or major events, or timing traffic flow.
- Deploying Assets—Any abandoned vehicles, stockpiling of suspicious materials, or persons being deployed near a key facility or major event.

Impersonation Threat Guidance

The Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC) learns weekly of incidents of first responder impersonation nationwide. While law enforcement authorities are justifiably concerned because many suspects are police impersonators in possession of items such as police badges, ID cards, uniforms, batons, handcuffs, gun belts, tasers, and light bars, other Emergency Services Sector (ESS) departments also are affected. Last week, the EMR-ISAC wrote of another incident of a cloned ambulance.

Regardless of the type of emergency responder being impersonated, the EMR-ISAC recognizes a growing threat to the critical infrastructures of communities and their emergency departments. This matter is particularly challenging for several reasons: a lot of authentic first responder paraphernalia can be obtained via internet sales and some local shops, many of the items are legally obtainable by non-emergency personnel, authentic accouterments and copy-cat accessories are frequently indistinguishable, and because too many incidents of successful impersonation are not reported.

Concerns by the National Association of Emergency Medical Technicians (NAEMT) warranted a re-issue of its "Security Alert for EMS Vehicles and Uniforms." This was done to encourage administrators to review existing security measures to prevent unauthorized use of vehicles or uniforms that would allow individuals to portray themselves as EMS personnel, and also to ensure ESS personnel safety. According to the NAEMT, organizations should consider adopting the following initial steps for their operations security assessment:

- Account for all vehicles (marked and unmarked), including tracking vehicles that are in service, out of service (e.g., reserve status, off-service repair status) and those going to salvage.
- Avoid leaving vehicles unattended when running or with keys left in the ignition.
- Track vehicle access by ensuring that out-of-service vehicles at stations are secured in a manner that significantly increases the difficulty of unauthorized access and use.
- Conduct routine and random vehicle audits and key inventories, and take requisite security corrective measures for unaccounted keys.
- Ensure that vehicles off premises for service are accounted for, especially when not in direct possession of the responsible organization. This includes government-based repair facilities, and contracted vendor services that require the vehicle to be shipped off site.
- Discuss compliance expectations with repair facilities and vendors to confirm that they understand the need to secure the vehicles indoors overnight when facility is closed, not leave keys in vehicles, and not allow vehicles to be taken off premises for any reason other than directly related to the repair and return of the unit to the owning organization.
- Report to the responsible organization and law enforcement officials any unusual interest in the vehicle while in the possession of a repair facility.
- Strip agency identifying markings from decommissioned vehicles slated for resale (unless to another bona fide emergency response organization), or vehicles scheduled for salvage. Removing emergency warning devices and other markings is strongly encouraged.
- Safeguard agency patches and ID cards to ensure defense against unauthorized access.
- Adopt counterfeit-resistant identification credentials that incorporate photos of authorized members.
- Provide alerts to uniform store vendors of the need to establish and verify the identity of individuals seeking to purchase uniform items by verifying agency identification credentials.
- Hold security briefings to inform personnel of present or emerging threats to their safety or the integrity of the mission.

Readers who are not NAEMT members can view the full alert here (PDF, 28 Kb).

Chem/Bio Quick Reference Guides

Quick Response Guides for numerous chemical and biological hazards can be downloaded now at the U.S. National Response Team (NRT) Web site.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) examined the guides and found they include useful protection and survival guidance for Emergency Services Sector (ESS) personnel. Each guide is formatted as a two-sided single page that displays 10 categories of information (e.g., agent characteristics, release scenarios, health effects, effect levels, field detection, etc.) with the greatest emphasis placed on personal safety: concerns, medical surveillance, first aid/decontamination, and personal protective equipment.

Chemical guides are available for Soman, Cyclosarin, Sulfur Mustard, VX, Tabun, and Sarin. Biological guides for anthrax, plague, Tularemia, Lassa Fever, Ebola, Marburg and Venezuelan Hemorrhagic Fevers, Brucella, Botulinum Toxin, and Tick-Borne Encephalitis are among those that can be downloaded

at the NRT Web site. The guides are located under the web site's "Hot Topics and Current Events" section. The EMR-ISAC notes the release of the chem/bio guides in the same timeframe as news of a posting in a jihadi Internet forum on detailed descriptions of anthrax production techniques intended to assist our enemies in producing biological weapons.

Updated ESS Rehabilitation Manual

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) was notified this week that the U.S. Fire Administration (USFA), in conjunction with the International Association of Fire Fighters (IAFF), released the updated and revised "Emergency Incident Rehabilitation" Manual that addresses ways to better protect Emergency Services Sector (ESS) personnel, the most critical of ESS infrastructures.

Emergency responder rehabilitation is designed to ensure that the physical and mental well-being of members operating at emergency scenes or training exercises do not deteriorate to the point where their safety is affected. The updated manual covers laws, standards, and guidelines that pertain to rehabilitation (e.g., OSHA, NIOSH, and NFPA). There are separate chapters devoted to heat and cold stress, and others that address establishing and operating a rehabilitation area, caring for personnel during rehab operations, and post-incident rehab considerations. One of the manual's two appendices is a Fire Department Standard Operating Procedure (SOP) for Emergency Incident Rehabilitation that could help guide departments that do not already have a rehab SOP in place.

"Effective emergency incident rehabilitation is an important facet of firefighter health and safety," said U.S. Fire Administrator Gregory Cade. The EMR-ISAC encourages ESS personnel to review and download the updated document (PDF, 5.6 Mm, 174 pp.).

Reporting Notice

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to DHS and/or the FBI. The DHS National Operation Center (NOC) can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@dhs.gov.

The FBI regional phone numbers can be found online at www.fbi.gov/contact/fo/fo.htm.

For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov.

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