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

INFOGRAM 26-08 July 10, 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.

Physical Security Planning

Recently, a security firm tested the physical security of numerous public and private organizations at several U.S. locations. Sometimes using uniform components from surplus stores and forged identification badges, the researchers were able to gain access to facilities 98 percent of the time. Access was granted without an escort on many occasions even when the test team members had very obvious errors to the clothing they were wearing, the identification they were carrying, and the explanations they were giving.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) acknowledges that Emergency Services Sector (ESS) personnel are typically very helpful and accommodating. Outstanding service to the community and its citizens is abundantly prevalent among first responders. Unfortunately, current realities make these positive mannerisms a potential vulnerability that provides significant advantages to those planning thefts or terrorist attacks.

Recognizing the interdependent relationship between critical infrastructure protection (CIP) and physical security, the EMR-ISAC examined the basic measures of a time-efficient, cost-effective, and common sense approach to physical security by ESS departments and agencies. The following is a summary of preventive actions from various sources for the consideration of ESS leaders responsible for any type of physical location:

- Acquire the assistance of a physical security specialist (usually from a law enforcement agency) to conduct annual physical security vulnerability assessments to determine where improvements are needed.
- Randomly inspect the security and condition of all facilities, storage areas, and HVAC systems.
- Increase observation and scrutiny of all facilities, storage, and surrounding areas.
- Keep all doors (including apparatus bay doors) and windows closed and locked unless these access points are continuously monitored so intruders can be immediately intercepted.
- Use appropriate locking systems for all access points (e.g., single cylinder locks for solid core doors and double cylinder locks for doors with glass).
- Obtain a monitored security alert system for buildings, storage areas, etc., that are not always occupied and in regular use.
- Guarantee that all apparatus, vehicles, and equipment maintained in exterior parking or storage areas are always locked when unattended.
- Periodically test security systems, back-up power sources, and emergency communications.
- Initiate and enforce a reliable identification system for department personnel and property.
- Develop inspection practices for incoming deliveries including postal packages and mail.
- Screen all visitors (including vendors) and deny entry to anyone who refuses inspection.
- Implement a dependable visitor/vendor identification and accountability system that includes escorting non-department personnel as much as practicable.
- Restrict access to communication centers and equipment including computer systems and networks to the few essential department personnel and authorized technicians.
- Prepare an SOP containing the organization's physical security policy and practices.
- Train department personnel regarding the application and enforcement of all physical security measures.

Threat Advisory System Response Guideline

The American Society for Industrial Security (ASIS) recently released the second edition of the "Threat Advisory System Response Guideline." ASIS developed the Guideline to provide organizations with security measures they might implement during elevated alert levels announced by the Department of Homeland Security (DHS). The Guideline is divided into four major sections that correspond to threat levels of the DHS Homeland Security Advisory System. Each section includes three subcategories: emergency response, personnel protection, and physical protection.

When reviewing the Guideline, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) learned that the document is a quality tool for Emergency Services Sector (ESS) departments and agencies. The document will enable ESS organizations to decide upon and provide a security architecture characterized by appropriate awareness, prevention, preparedness, and response to changes in threat conditions. Its detailed worksheet format will help decision makers determine those steps that apply to specific security environments.

ASIS developed the Guideline as an initiative to provide private business and industry a methodology for prompt consideration of possible actions that could be implemented based upon changes in the Homeland Security Advisory System. The document's overarching objective is to balance the need for a process both applicable and understandable to a large portion of the private sector, while also providing sufficient detail to be of practical use to the organization.

The EMR-ISAC suggests that this Guideline has planning and operating value for emergency services organizations. Therefore, it can be seen and downloaded at the following link: http://www.asisonline.org/guidelines/guidelinesthreat.pdf (856 KB, 36 pp.).

Digital Radio Transmissions

The International Association of Fire Chiefs (IAFC) recently released "Interim Report and Recommendations: Fireground Noise and Digital Radio Transmissions." The report is the result of a project by the IAFC's Digital Problem Working Group to determine the extent of radio transmission problems associated with fireground noise. It is based on a year of study begun after an IAFC member alert in March 2007 that responders were experiencing unintelligible audio communications while using digital two-way portable radios in close proximity to the low-pressure alarm of their self-contained breathing apparatus (SCBA).

According to the report, "There are many significant factors that contribute to the challenges of present-day public-safety communications, and they include but aren't limited to the increased number of radios operating at an emergency scene, radio complexity, inadequate radio training, unique traits of trunked radio systems, in-building coverage, and audio intelligibility in high-noise environments."

The report states that Emergency Services Sector (ESS) personnel, "routinely work in and cannot avoid high-noise environments…." It also asserts: "Any improvements that recognize and can improve the public-safety working environment and increase communications intelligibility should be considered a high priority." Results of independent tests by two national laboratories formed the basis for initial best practices for portable radios, and technical and procedural best practices.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) notes the report additionally includes the following ESS leadership recommendations:

- Train personnel to properly use the assigned radio equipment in conjunction with all components of the protective ensemble.
- Develop standards and guidelines for scenario-based user training utilizing their communication equipment.
- Involve responder organizations from the beginning in the design and development of requirements for any communication-system implementation.
- Verify that incident commanders evaluate background noise in the environment as a safety consideration in task assignments.

- Require system managers and users to work with their vendors to ensure that their radios and accessories are compatible and configured with the optimal system settings to maximize audio intelligibility in high-noise environments.
- Consider, when practical, the use of accessories, such as speaker microphones, throat microphones and in-ear microphones to reduce the impact of background noise.
- Evaluate communication-equipment integration requirements in the design of SCBA and personal alert safety system (PASS) and other equipment and systems that contribute to the firefighter's protective envelope.

The initial best practices for portable radios and technical and procedural best practices can be viewed at http://www.iafc.org/associations/4685/files/digProb_PortableRadioBestPractices.pdf (106 KB, 21 pp.). Visit the following link to read or download the interim report: http://www.iafc.org/associations/4685/files/digProj_DPWGinterimReport.pdf (63 KB, 10 pp.).

Ethanol Update

A new shipping description for gasoline/ethanol fuel blends intends to enhance personnel protection and effective response for Emergency Services Sector (ESS) departments and agencies. The U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration (PHMSA) Final Rule amending the Hazardous Materials Regulations (HMR 49 CFR parts 171-180) becomes effective on 1 October 2008.

As part of the new description, ethanol mixtures with more than 10 percent ethanol will display the United Nations (UN) identification number UN 3475, II, "to enable emergency responders to quickly identify whether an ethanol fuel blend is present and minimize confusion as to appropriate response measures," according to the full text of the Final Rule, published in the 28 January 2008 Federal Register (http://hazmat.dot.gov/regs/rules/final/73fr/docs/73fr-4699.pdf). The new shipping description also is included in the 2008 edition of the "Emergency Response Guide."

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) examined resources offered by the Ethanol Emergency Response Coalition (EERC), comprised of organizations that represent emergency responders, the fuel industry, and testing organizations. Available at no charge at the EERC web site are a ready-to-use instructor guide and participant manual for the "Responding to Ethanol Incidents" course, a 19-minute ethanol incident response video, EERC brochure, and additional materials. Visitors to the site can subscribe to the EERC's distribution list to receive regular information updates at http://www.ethanolresponse.com/resources.html. For a state-by-state list of ethanol plants, see http://www.dtnethanolcenter.com/index.cfm?show=47&mid=48.

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