



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

INFOGRAM 13-10

April 1, 2010

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.

Preventing Thefts at Fire and EMS Stations

Thieves recently broke into two fire stations and stole narcotics from locked cabinets within ambulances, according to an [article](#) by The Denver Post. The chief officers of victimized departments shared that similar station break-ins and thefts occurred at no less than four other fire departments in the Denver metropolitan area. "The would-be thieves were either watching the station or were listening to scanners and knew the moment the crew was gone." The deputy chief of one of these departments stated: "This is compromising the public safety services we provide, and the perpetrators need to be stopped."

Recognizing the interdependent relationship between critical infrastructure protection (CIP) and physical security, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) examined the basic measures of a time-efficient, cost-effective, and common sense approach to bolster physical security by Emergency Services Sector (ESS) department and agencies, and to eliminate the thefts discussed in the preceding paragraph. The following is a summary of preventive actions from various sources for the consideration of ESS leaders responsible for any type of physical location:

- Inspect randomly the security and condition of all facilities and storage areas.
- Keep all doors and windows closed and locked unless continuously monitored.
- Use appropriate locking systems for all access points including cabinets containing medication.
- Obtain a monitored security alert system for locations not always occupied and in regular use.
- Avoid providing security codes or combinations to unauthorized persons.
- Change security codes or combinations at frequent intervals.
- Guarantee vehicles, apparatus, and equipment at exterior sites are always locked when unattended.
- Initiate and enforce a reliable identification system for department personnel and property.
- Conduct a regular inventory inspection of emergency equipment and medications.
- Prepare a Standard Operating Procedure containing physical security policies and practices.

The EMR-ISAC offers some guidance for improving the physical security of emergency facilities, vehicles, and equipment, which can be seen at the following documents: [Department of Homeland Security Physical Security Performance Measures](#) (PDF, 631 KB), and the [U.S. Geological Survey Physical Security Handbook](#).

Social Networking and OPSEC

Social networking sites (SNS) such as Twitter, Facebook, MySpace, and others are very popular for establishing professional connections as well as for social relationships and personal purposes. The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) observed that these Web applications connect people and information in spontaneous, interactive ways, which can be quick, useful, and fun. However, according to a [US-CERT Cyber Security Tip](#), "the nature of these sites introduces security risks."

In its presentation, "[Social Networking and the OPSEC Threat I](#)," the [Operations Security \(OPSEC\) Professional's Association](#) cautioned that some malicious people are drawn to SNS because of the accessibility, availability, and amount of professional and personal information. These sites can provide adversaries such as miscreants, criminals, and terrorists with critical information needed to disrupt your mission, harm you physically or financially, or disparage you in various ways.

To protect yourself, family, friends, and organization, the [Interagency Operations Security Support Staff \(IOSS\)](#) listed in several different briefings the following things that should not be shared on social networking sites:

- Names and photos of you, family, friends, and co-workers.
- Home addresses and phone numbers.
- Usernames, passwords, and network details.
- Job titles, locations, salaries, and security clearances.
- Social security numbers, credit card numbers, and banking information.
- Home and business physical security measures and logistics matters.
- Business mission capabilities and limitations.
- Professional and personal schedules and itineraries.
- Hobbies, likes, dislikes, etc.
- Permissions for individuals who are not known and trusted.

Practicing OPSEC, which is the protection of sensitive, but unclassified information, can help you make informed, reliable decisions regarding the use of SNS. The EMR-ISAC recommends the use of the [IOSS Safety Checklist](#) (PDF, 149 KB) to reduce or eliminate the possibility of being victimized when enjoying the benefits of SNS.

TRANSCAER Update

Transportation Community Awareness and Emergency Response ([TRANSCAER](#)) is a voluntary national outreach effort that focuses on assisting communities to prepare for and respond to possible hazardous material (HazMat) transportation incidents. "TRANSCAER members consist of volunteer representatives from the chemical manufacturing, transportation, distributor, and emergency response industries, as well as the government." It promotes safe transportation and handling of HazMat, educates and assists communities near major transportation routes about HazMat, and aids community emergency response planning for HazMat transport incidents.

When examining their [brochure](#) (PDF, 943 KB), the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) verified that TRANSCAER provides the following specific services:

- Planning assistance to local communities for HazMat emergencies.
- Classroom and hands-on training.
- Drills and exercises to improve the response and handling of HazMat incidents.
- HazMat safety training to communities in states along rail corridors ("Whistle Stop Tours").
- Reference and training materials about chemicals and transport equipment.
- National conferences and workshops sharing best practices, new programs, and resources.
- State coordinators to help local responders connect with chemical and HazMat carriers and shippers.

The TRANSCAER Outreach and Special Programs Director informed the EMR-ISAC that the organization delivers high-quality training at no expense to Emergency Services Sector personnel or their departments. Visit their [web site](#) to acquire more information about TRANSCAER.

Caution at Vehicle Fires

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) learned the U.S. Fire Administration (USFA) published a “Highway Vehicle Fires” [Topical Report](#) in October 2008. The document provided the findings of the [National Fire Incident Reporting System](#) revealing approximately one in six fires was a highway vehicle fire between 2004 and 2006, resulting in about 258,500 responses by firefighters.

According to an [article](#) in Fire Engineering, “vehicle fires continue to remain an integral part of fire department responses.” The author stated that there has been a downward trend in the number of vehicle fires over the past decade; however, the hazards associated with these incidents have been consistently elevated as vehicles have become more technologically sophisticated. He further indicated that a vehicle fire can produce toxic smoke, launch projectiles, and generate heat upward to 1,500 degrees.

For example, the EMR-ISAC noted the outcome of a [fire department response](#) to a vehicle fire last month. As firefighters doused the flames an explosion occurred when water hit burning magnesium. Protective gear saved them from serious injury. The incident reinforced the necessity for emergency responders to follow personal protective equipment safety practices when extinguishing vehicle fires, including full protective clothing with self-contained breathing apparatus.

Considering other similar experiences throughout the nation, the EMR-ISAC agrees that vehicle fires should not be routine, but should be handled in a cautious, safe manner commensurate with a “size-up” and risk assessment to ensure the protection of responders and success of the mission. See the [paper](#) “Over-Aggressive Attacks on Vehicle Fires” for more information on this subject.

DISCLAIMER OF ENDORSEMENT

The U.S. Fire Administration/EMR-ISAC does not endorse the organizations sponsoring linked web sites, and does not endorse the views they express or the products/services they offer.

FAIR USE NOTICE

This INFOGRAM may contain copyrighted material that was not specifically authorized by the copyright owner. EMR-ISAC personnel believe this constitutes “fair use” of copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use copyrighted material contained within this document for your own purposes that go beyond “fair use,” you must obtain permission from the copyright owner.

REPORTING 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: 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/emr-isac, Mail: E-108, 16825 South Seton Avenue, Emmitsburg, MD 21727