



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

INFOGRAM 49-09

December 17, 2009

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.

Suspicious Holiday Cards, Letters, and Packages

During this holiday season, it is reasonable to expect that some Emergency Service Sector (ESS) departments and agencies may receive cards, letters, and packages recognizing the service and sacrifices of local emergency responders. Unfortunately, the possibility exists that the season's greetings could contain explosives, chemicals, or biological agents. Although there is no known threat against ESS organizations, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) shares the following [typical characteristics](#) of mail and packages that should trigger suspicion:

- Sent by an unexpected or an unknown person or source.
- Contain no return address or an address that cannot be verified as legitimate.
- Have protruding wires or aluminum foil, strange odors or stains.
- Show a city or state in the postmark that does not match the return address.
- Are of unusual weight given their size, or are lopsided or oddly shaped.
- Marked with threatening language.
- Labeled in an inappropriate or unusual manner.
- Include excessive postage or packaging material, such as masking tape and string.
- Contain misspellings or common words.
- Addressed to someone no longer with the organization or used other outdated information.
- Titled incorrectly or without a name.
- Are not addressed to a specific person.
- Have hand-written or poorly typed addresses.

See the following web sites for additional information about suspicious mail:

- [Federal Bureau of Investigation](#)
- [Centers for Disease Control and Prevention](#) (PDF, 241 Kb)

FEMA Disaster Information Sources

In its Critical Infrastructure Protection (CIP) Process [Job Aid](#) (PDF, 4.6 Mb), the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) explained that the second step of the CIP process is to determine the threats against critical infrastructures. American history and experience substantiates that deliberate, natural, and accidental incidents can be serious threats to state and local critical infrastructures.

The Federal Emergency Management Agency (FEMA) provides information on seventeen different types of disasters and hazards on its Get Disaster Information [web site](#). Understanding past declared disasters could assist state and local leaders in planning and rehearsing emergency preparedness plans, including protection measures or resilience actions for what cannot be protected. FEMA also offers additional reference information on its [web site](#) for Declared Disasters by Year or State.

The ability to survive man-made and natural disasters and restore normal operations shortly after a catastrophe results from comprehensive, pre-event, all-hazards research and planning. The EMR-ISAC acknowledges that consulting the two aforementioned FEMA web sites can potentially impart current threat perspectives and historical insights that could enhance the reliability and effectiveness of state and local preparedness planning.

Methanol Hazards

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) examined the [Methanol Safe Handling Manual](#) (PDF, 918.7 Kb) published by the [Methanol Institute](#). According to the Methanol Institute, the manual was designed to be a resource for current information on methanol's properties, potential environmental and health and safety hazards, safe handling practices, emergency response procedures, fire safety, and risk communication.

Known as "wood alcohol," methanol is a clear, flammable liquid with a faintly sweet pungent odor. Methanol occurs naturally and is produced synthetically. It is used in multiple products including plastics, paint, construction materials, as well as fuel in some race cars, monster trucks, go-carts, and model planes, boats, and cars. In addition, methanol is utilized for denitrification (i.e., nitrogen removal) in municipal wastewater treatment plants and can also be used as turbine fuel for electric power generation.

Ingestion can cause irreversible injury to the nervous system, blindness or death. Methanol causes eye, respiratory system, and skin irritation. The manual explains that methanol fires generate less heat, have nearly invisible flames in daylight, and produces very little smoke. Considering the risks, first responders may find the [Methanol Material Safety Data Sheet](#) (PDF, 33.4 Kb) a quick reference and companion to the Methanol Safe Handling Manual.

The EMR-ISAC confirmed that the Methanol Institute is offering a free [DVD](#) that can be another resource for training. The DVD discusses basic physical components, key risks of handling methanol, ways to minimize exposure, fire and release into the environment, and event response. For general operating procedures, first responders can also refer to the [Emergency Response Guidebook, guide #131](#).

Threat Detection and Reaction

The "[Soft Target Awareness: Threat Awareness and Detection for Retail and Shopping Center Staff](#)" training video was developed by the Department of Homeland Security Office of Bombing Prevention and the Commercial Facilities Sector to provide information for retail staff to understand how to identify and report unusual activities and threats in a timely manner. The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) recognizes that the Emergency Services Sector organizations might find relevance in the contents of this video when working with shopping centers, malls, or retail facilities.

This training tool uses case studies and best practices to explain suspicious behavior and items, how to reduce the vulnerability of an active shooter threat to a soft target, and the appropriate actions to take if employees notice suspicious activities.

The EMR-ISAC observed the following three key areas presented in the video:

- Recognize the threat from suspicious behavior or activities.
- Report the threat to appropriate personnel.
- React to the threat by knowing what to do.

The presentation requires Adobe Acrobat software and will initiate upon accessing the video. It is self paced and can be played for individual use or any size group. The video will be available until February.

Holiday Vigilance

As we gather with family and friends between 24 December and 3 January, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) staff wish all members of the Emergency Services Sector (ESS) a very happy, safe, and peaceful holiday season. It was an honor and pleasure to provide sector personnel with infrastructure protection and resilience information during this past year.

At this festive time of the year, ESS leaders, owners, and operators comprehend that the critical infrastructures (i.e., personnel, physical assets, and communication/cyber systems) upon which our loved ones and citizens depend must remain intact and operational without incapacitation or destruction by deliberate, natural, or accidental causes. Therefore, while our thoughts and attention turn to possible travel and celebrations, the EMR-ISAC acknowledges that continued vigilance is necessary to ensure the survivability, continuity, and responsiveness of emergency departments and agencies.

Several domestic and international incidents in 2009 have been chilling reminders that our adversaries—frequently weather—do not rest, but persist to threaten infrastructures, exploit vulnerabilities, and test protective measures. Hence, persistent and effective preparations and vigilance is a harsh reality to deter or prevent similar events from occurring or reoccurring in the United States.

NOTE: There will be no INFOGRAM published on 24 and 31 December. Nevertheless, the EMR-ISAC will continue to monitor events during the holidays and disseminate any credible information regarding man-made emergencies or natural disasters. The next INFOGRAM will be dated 7 January 2010.

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