



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

INFOGRAM 43-08

November 6, 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.

Identifying Suspicious Activity

Many actions by individuals can be considered suspect; however, questionable photography is among the more frequently reported activities according to state and local fusion centers. When consulting several fusion centers, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) learned that suspicious activity reporting such as dubious photography provides valuable information for analysis and further investigation if warranted.

The EMR-ISAC discerned that only a small number of reported suspicious activities actually receive further investigation. According to law enforcement authorities, a lack of understanding regarding what constitutes a questionable action is the major reason for the small number of investigations. They explain that “being able to distinguish suspicious from legitimate activities adds a perspective that saves resources for genuine threats.”

While it does not necessarily indicate terrorist behavior, police sources elaborate that photography in conjunction with particular behaviors should increase suspicion. Therefore, the Joint Regional Intelligence Center offers the following suspicious activities, which were abridged by the EMR-ISAC for the assistance of Emergency Services Sector personnel and the protection of their infrastructures:

- Recording notes or making drawings at or nearby sensitive areas.
- Using techniques such as doubling back, changing appearance, or driving evasively.
- Taking apparent measurements between entrances, security points, and around a perimeter.
- Trespassing or trying to access sensitive or unauthorized areas.
- Questioning sector personnel about sensitive subjects (e.g., personnel, plans, operations).
- Photographing items with no apparent aesthetic value (e.g., personnel, equipment, systems).
- Capturing pictures of items or at odd times that are inconsistent with being a tourist, artist, etc.
- Wearing clothing, using photo equipment, or behaving in a manner that is inconsistent with the photographer’s explanation.
- Being sly or evasive such as refusing to show pictures taken on a digital camera.
- Returning to the same location to take photos after being instructed not to do so.

More information regarding suspicious activity and awareness can be seen at the following links:

- http://www.fbi.gov/page2/july06/protect_workplace071006.htm.
- <http://www.pa-aware.org/protecting-your-community/suspicious-activity.asp>.

The Insider Threat

According to a National Infrastructure Advisory Council (NIAC) report released in April 2008, insider threats exist for all American organizations and communities. Through the Department of Homeland Security Secretary, the NIAC provides the President of the United States with advice on the security of the critical infrastructure sectors and their information systems.

In its report, the NIAC explained that the threat to local critical infrastructures involves one or more individuals with access to physical assets, communication/cyber systems, and services with the intent to cause harm. “Insider betrayals include a broad range of actions, from secretive acts of theft or subtle forms of sabotage to more aggressive and overt forms of vengeance, violence, and destruction.”

Having reviewed the NIAC document, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) shares the following abbreviated findings from the NIAC and other sources for consideration by the leadership of Emergency Services Sector departments and agencies:

- Understand the insider threat and increase efforts to mitigate or eliminate it.
- Improve employee screening and risk assessment by access to the best available historical records.
- Initiate programs to enhance employee ethics, accountability, and loyalty.
- Establish a priority to maintain current information technology and network best practices.
- Enforce identification checks of all personnel entering any department or agency facility.
- Prohibit entry of unauthorized personnel to data and information processing sites.
- Secure contracts with known and reputable vendors who hire dependable, bonded personnel.

The NIAC report can be seen and downloaded from the following link (400 KB, 56 pp.):
http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.

Biological Threat Model Procedures

The International Association of Fire Chiefs (IAFC) and the Federal Bureau of Investigation (FBI) Hazardous Materials Response Unit collaborated to produce model procedures for first-arriving responders to incidents that involve packages suspected of containing biologically threatening substances.

“Model Procedures for Responding to a Package with Suspicion of a Biological Threat,” released last month, acknowledges that Emergency Services Sector (ESS) departments and agencies across the nation have taken independent action to address these incidents, but the actions lack uniformity. The document was created to complement the concepts of unified command, promote interoperability, and generate standard operating guidelines. Definitions, identification and assessment of biological threats, and decontamination guidelines for exposed personnel are presented. Appendix topics include media coverage, identifying suspicious packages, additional information on biological weapons, and a sample equipment list for responders.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) notes that the model provides a framework for building a local protocol tailored to individual communities, lending universal applicability for all types of departments in all types of communities. While it specifically addresses biological threats delivered through a point source such as those that could arrive in the mail or similar delivery systems, many of the procedures would be similar for any bio-terror response. The document (161 KB, 20 pp.) can be viewed and downloaded at
http://www.iafc.org/associations/4685/files/haz_IAFCmodelproceduresforbiohazardresponse.pdf

Chemical and Radiologic Threats

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) examined the recently released “Response Guide for Chemical and Radiologic Threats: Are We Ready,” a special supplement of awareness and survival information targeted to Emergency Services Sector (ESS) members.

The supplement looks at nerve agents, cyanide poisoning, mustard gas, and lessons learned from the 2006 murder by poisoning (with radioactive Polonium-210) of former Soviet spy Alexander Litvinenko. Polonium-210 is considered one of the most hazardous of all radioactive materials. Signs and symptoms of possible attack, treatment information, and response considerations are offered in each chapter.

The first chapter, "Don't Get Caught...in a state of complacency," describes an incident in which information conveyed by a 9-1-1 dispatcher to first-arriving responders included a warning that organophosphorus chemicals might be involved, which was instrumental in preventing deaths and injuries. The response included dispatching the city's hazardous materials team to the receiving hospital to manage potential exposure issues, advise hospital staff about managing the patient's highly toxic body fluids, and decontaminate the ambulance.

The jems.com supplement (~7 MB, 23 pp.) can be viewed and downloaded at http://www.jems.com/news_and_articles/special_topics/terrorism_preparedness.html. Also available at the link are a decontamination equipment list, general guidelines for mustard gas responses, and information about Levels 1, 2, and 3, radiation detection equipment for responders.

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: <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