



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

INFOGRAM 32-08

August 21, 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.

Period of Heightened Alert

The Department of Homeland Security (DHS) established a Period of Heightened Alert for the high-profile events that include the Democratic National Convention, Republican National Convention, Election Day, and Presidential Inauguration. Although DHS maintains there is no specific or credible threat against the United States, counterterrorism officials expressed concern that the nation is more vulnerable to terrorist attacks particularly between August 2008 and January 2009. Presently, DHS has no plans to raise the National Security Advisory System Level from YELLOW (Elevated) to ORANGE (High).

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) noted that the six-month period of time in which these events of national significance will occur is a “window of vulnerability.” Terrorism analysts speculate that possible targets could include all the political gatherings (e.g., conventions, meetings, rallies, speeches, formals, parties, etc.) associated with selecting and electing a new Presidential Administration. These specialists fear transnational and domestic terrorists, anarchists, and extremist groups will attempt actions that drain Emergency Services Sector (ESS) resources, disrupt planned events, target political personalities, and capture media attention.

Throughout this period of vulnerability, the DHS will increase security at the various venues that potentially represent appealing targets to terrorists. Despite unprecedented security arrangements, the EMR-ISAC suggests heightened awareness and emergency operations planning by ESS departments and agencies with these special events at or adjacent to their jurisdictions. Additionally, affected ESS organizations should also consider establishing effective contact with their local Joint Terrorism Task Force (JTTF).

According to reputable security specialists, “Terrorists recognize that by disrupting response and recovery operations, additional lives are likely to be lost, and the psychological impact of the attack will be greater.” More information about increased vigilance can be seen in the Washington Post article at: <http://www.washingtonpost.com/wp-dyn/content/article/2008/07/28/AR2008072802544.html>.

Cloned Vehicle Threat Increases

Research by the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) substantiates that the term “cloned vehicle” pertains to cosmetically altered vehicles made to look like legitimate emergency or commercial vehicles, but also applies to vehicles with fictitious titles and vehicle identification numbers. An investigation by *Homeland Security Today* disclosed that “cloned vehicles” have been reported from Oregon to Georgia. Completely cloned 18-wheelers disguised as Wal-Mart trucks have been impounded in Oklahoma, Texas, Kansas, Arkansas, and Missouri, according to law enforcement officials.

Within the United States, the potential exists for the use of cloned vehicles for terrorist activities ranging from surveillance and preplanning to an actual terrorist attack as has occurred in other nations. Because of this viable threat, the EMR-ISAC recommends that Emergency Services Sector (ESS) personnel develop the ability to detect “cloned vehicles” and distinguish them from genuine emergency and commercial vehicles.

To assist ESS departments and agencies, the EMR-ISAC offers the following additional suggestions to prepare emergency responders for this increased threat:

- Learn about the technology and resources to develop “cloned vehicles.”
- Familiarize with the actual methods and materials used to create “cloned vehicles.”
- Pay attention to delivery, service, and utility vehicles while performing duties.
- Know how to verify the official markings on government and military vehicles.
- Be able to locate concealed illicit items, particularly those harmful to responders and citizens.
- Promote the creation of laws or statutes that criminalize the development and use of “cloned vehicles.”

Additional information about the proliferation of “cloned vehicles” can be seen at:
https://www.nicb.org/cps/rde/xbcr/nicb/13734_VehicleCloning_Eng.pdf.

Bloodborne Pathogens after Mass-Casualty Events

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) examined updated guidance from the Centers for Disease Control and Prevention (CDC) intended to protect Emergency Services Sector (ESS) personnel after bombing incidents and also to guide their treatment of victims.

“Recommendations for Postexposure Interventions to Prevent Infection with Hepatitis B Virus, Hepatitis C Virus, or Human Immunodeficiency Virus, and Tetanus in Persons Wounded During Bombings and Other Mass-Casualty Events—United States, 2008,” was revised, in part, based on reports from the Israeli health ministry that in August 2001, tissue from two suicide bombers tested positive for evidence of hepatitis B virus (HBV). In 2002, it found evidence of HBV in a bone fragment that had implanted into a bombing survivor. Traumatically implanted bone fragments were removed from five survivors of the 2005 London bombings.

ESS personnel, first on the scene of bombing and other mass-casualty events, face personal injury and risk exposure to infection from HBV, hepatitis C virus (HCV), or human immunodeficiency virus (HIV) and tetanus through contact with wounds from injured persons (including suicide bombers and bombing casualties).

The report states that emergency responders and health-care providers in the U.S. need uniform guidance on prophylactic interventions appropriate for persons injured in bombings and other events resulting in mass casualties. The recommendations in the report pertain only to bombings and mass-casualty events, and are not meant to supplant existing recommendations for other settings. Further, the recommendations are limited to issues regarding initial postexposure management for bloodborne pathogens and tetanus prophylaxis. Other prophylactic measures that might be appropriate (e.g., use of antibiotics for the prevention of bacterial infection) are not discussed.

Responders, particularly EMS personnel, may review the updated guidance at
<http://www.cdc.gov/MMWR/preview/mmwrhtml/rr5706a1.html>.

EMR-ISAC CIP INFOGRAM Archives

Responding to requests from Emergency Services Sector (ESS) chief officers, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) completed arrangements for an electronic search tool at the web site of the U.S. Fire Administration (USFA). Emergency Services Sector personnel can now use this new feature to perform a title/topic/subject/key word search of all EMR-ISAC weekly INFOGRAMs published from 2001 through the present.

Interested individuals can acquire information and resources on critical infrastructure protection and resilience (CIP/CIR), the threats to and vulnerabilities of ESS infrastructures, and hundreds of related topics, as found in over 1,500 articles contained in more than 380 INFOGRAM issues. After clicking on the following link, scroll down to “Search INFOGRAM Archive,” and enter the desired title/topic/subject/key word. The results will be rapidly provided. The URL to search is <http://www.usfa.dhs.gov/fireservice/subjects/emr-isac/infograms/index.shtm>.

Also in response to a request, the EMR-ISAC offers a PDF version of each week’s INFOGRAM, which is available at the above link by selecting the desired issue and clicking the Adobe Acrobat symbol. PDF versions can be obtained at this EMR-ISAC page of the USFA web site for INFOGRAMs dated 28 February 2008 and after.

The EMR-ISAC appreciates the ongoing efforts of the USFA webmaster to provide a quality experience for EMR-ISAC web site end users, as well as the constructive feedback from INFOGRAM readers.

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