



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

INFOGRAM 41-10

October 14, 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.

Destroying Obsolete Electronic Devices

(Source: Government Security News)

According to page 26 of the [September 2010 issue](#) of [Government Security News](#), “when a digital file is deleted from a computer, the information actually remains on the hard drive, as do deleted e-mail messages and records of all online activity.” The article reminded the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) that despite deliberate efforts to delete information, an obsolete or unwanted hard drive, CD, and DVD can contain thousands of files, which can be recovered with sophisticated tools for the purpose of adversarial data collection, espionage, identity theft, etc.

The EMR-ISAC confirmed that computer hard disk drives, thumb/flash drives, memory cards, cell phones, BlackBerries, CDs and DVDs, floppy and zip disks, laser printers, and facsimile machines—all of which are used by Emergency Services Sector (ESS) departments and agencies—could be susceptible to data mining if merely discarded and not disposed of properly. The following methods can be used to thoroughly destroy the aforementioned items before being given away or thrown away:

- Shredding. Reducing items to small strips or particles (i.e., CDs and DVDs).
- Degaussing. Using powerful magnets to permanently eliminate data from magnetic media.
- Disintegration. Mechanically cutting items into the smallest pieces until unreconstructible.
- Declassification. Physically grinding the data-bearing surfaces from CDs and DVDs.
- Crushing. Subjecting items to extreme pressure with various items such as a hammer.

More information about destroying unwanted electronic devices can be found at the following links for the consideration and protection of ESS organizations:

- [Prepare Your Hard Drive for Disposal](#)
- [Drive Disposal Best Practices](#) (PDF, 40.74 KB)
- [How to Dispose of Computer Equipment](#)

Emergency Surge Modeling Tool

(Source: Agency for Healthcare Research and Quality)

The [Agency for Healthcare Research and Quality](#) (AHRQ), which is a component of the U.S. Department of Health & Human Services (HHS), recently announced that the [Hospital Surge Model](#) now allows users to estimate the resources needed to respond to emergencies involving improvised explosive devices, pneumonic plague, and foodborne botulism. The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) verified that this web-based interactive model presently includes a total of 13 scenarios on biological incidents and attacks ranging from pandemic influenza to a nuclear explosion.

Emergency managers and hospital planners can use the Hospital Surge Model to develop specific strategies to treat an influx of patients affected by these specific incidents. It will estimate, by day, the severity of injury and the number and flow of casualties needing medical attention for particular scenarios selected by users.

The Hospital Surge Model was developed by AHRQ in collaboration with HHS. The EMR-ISAC observed that more than 60 other AHRQ emergency preparedness [tools and resources](#) are currently available for community planning by Emergency Services Sector organizations.

Evacuation Planning Guide for Stadiums

(Source: Department of Homeland Security)

Throughout each year, America's sports venues (e.g., baseball and football stadiums, basketball complexes, hockey arenas, soccer fields) are in relatively constant use. Sometimes, these same locations are used for other purposes such as music concerts, religious gatherings, and political rallies. According to the Department of Homeland Security (DHS) "[Evacuation Planning Guide for Stadiums](#)" (PDF, 395 KB), an Evacuation Plan should be an essential component (i.e., appendix) of the stadium's Emergency Plan.

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) understands that to ensure a well managed and coordinated evacuation, stadium owners and operators must coordinate their evacuation plans with local, state, and if appropriate, federal authorities. The Guide indicates coordination is best accomplished through maintaining ongoing communications with local Emergency Services Sector (ESS) departments and agencies, planning for hazardous incidents, and training and exercising with the same ESS organizations to enhance a stadium's evacuation capability.

The EMR-ISAC noted that the Guide provides detail and structure for developing a comprehensive Evacuation Plan for an individual stadium or similar setting. Each section of the document contains subsection topics that include questions for consideration and statements for supporting actions. "The Evacuation Plan should reference the Emergency Plan whenever possible and should be consistent with local emergency response plans that include evacuation scenarios."

Emergency Communications Forum

(Source: DHS, Office of Emergency Communications)

The Department of Homeland Security (DHS) [Office of Emergency Communications](#) (OEC) notified the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) that the OEC released Volume III of the *Emergency Communications Forum* (ECF) [newsletter](#) (PDF, 1.04 MB). The ECF engages and informs emergency responders; policy makers; and federal, state, local, and tribal officials about issues and events that directly affect everyday nationwide emergency communications.

Volume III of the ECF newsletter highlights the work of emergency responders who supported the Gulf Coast oil spill and those who responded to the Tennessee floods in May. It also details the progress of the [National Emergency Communications Plan](#), since it was published in 2008, and provides an overview of the [statewide plan](#) workshops that were conducted in 50 states and territories in 2010.

The OEC invites interested personnel to subscribe to the ECF by sending e-mail to OEC@hq.dhs.gov. Those who wish to submit an article pertaining to emergency communications in the field, best practices, and lessons learned can send their information to the same electronic address.

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