



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

INFOGRAM 40-10

October 7, 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.*

Cybersecurity Month

(Source: Department of Homeland Security)

[Department of Homeland Security](#) (DHS) cybersecurity officials assert that the cyber threat to the critical infrastructures of the United States has become one of the most serious economic and national security challenges we face. They maintain that America's competitiveness and economic prosperity in the 21st century will depend on effective cybersecurity.

Considering the potential effects on the operations of Emergency Services Sector (ESS) departments and agencies from a power grid cyber attack, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) recognizes October 2010 as the seventh annual National Cybersecurity Awareness Month sponsored by DHS. To enhance the cybersecurity of ESS departments and agencies, there are a few steps that first responders can follow to protect personnel, physical assets, and communication/cyber systems when conducting business online for their emergency organizations.

The following procedures summarized by the EMR-ISAC may improve organizational cybersecurity and also demonstrate support for National Cybersecurity Awareness Month:

- Learn cybersecurity fundamentals and educate personnel who use organizational systems.
- Ensure anti-virus software and firewalls are installed, properly configured, and up-to-date.
- Update the operating system, critical program software, and web browsers.
- Back-up all important files on a removable disc and store it in a safe place.
- Enforce the use of strong passwords or strong authentication technology.

See the following recommended sites for more helpful information regarding cybersecurity:

- [National Cybersecurity Awareness Campaign](#)
- [OnGuardOnline.gov](#)
- [StaySafeOnline.org](#)
- [U.S. Computer Emergency Readiness Team](#)

Cyanide Awareness

(Source: Centers for Disease Control and Prevention)

According to the [Centers for Disease Control and Prevention](#) (CDC), cyanide is a rapidly acting and potentially deadly chemical that can exist as a colorless gas, such as hydrogen cyanide or cyanogen chloride, or in a crystal form such as sodium cyanide or potassium cyanide. It is widely used in the manufacture of paper, textiles, and plastics. The majority of cyanide produced in the United States is found in products used in building construction, interior decorations, or furnishings.

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) confirmed that the primary effect of cyanide on the human body is cell poisoning and cellular asphyxiation. All forms of cyanide can be toxic at high levels, but hydrogen cyanide is the deadliest form. It is especially fast-acting when inhaled, resulting in a variety of symptoms including an initial brief period of rapid and deep breathing or gasping, followed by a loss of consciousness, convulsions, cessation of breathing, and eventually death.

First responders are most likely to encounter cyanide compounds when responding to fires and hazardous material spills, or attending to victims of cyanide suicides. A victim of cyanide poisoning may present a physical hazard to those providing emergency care and transportation. Emergency medical personnel should use personal protective equipment (PPE) to shield themselves from the secondary cyanide hazards posed by victims and should follow the PPE recommendations and procedures of their respective organizations.

For more information about this hazard to ESS personnel, the EMR-ISAC offers the [website](#) of the Cyanide Poisoning Treatment Coalition.

Maintaining a Suspicious Attitude

(Source: FireRescue1.com)

As exemplified by an [article](#) in FireRescue1.com, open source reporting in recent months suggests that Emergency Services Sector (ESS) departments and agencies should ensure their personnel “keep a high index of suspicion when approaching even seemingly ‘routine’ incidents.” This suggestion was an outcome or lesson learned from the 1 May Times Square bomb plot in New York City.

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) understands that when responding to daily emergencies it is occasionally easy to forget the continued threat from domestic and transnational terrorists at home and abroad, as well as the necessity to remain vigilant in all circumstances. The effective response to the Times Square attempted bombing again demonstrated that ESS personnel remain on the front lines of the Global War on Terror, and can prevent or protect against criminal or terrorist activities if they maintain a suspicious attitude.

The actions of New York City first responders on 1 May are “an outstanding example of developing situational awareness and selecting the right strategic/tactical approach for addressing a suspicious situation.” In addition to extinguishing the fire, they appropriately considered the possibility of a secondary device, which is a popular tactic for targeting emergency responders in the Middle East.

The EMR-ISAC observed more information at [FireRescue1.com](#) regarding responder actions at the attempted New York City bombing last May.

2010 Critical Infrastructure Protection Congress

(Source: National Council of ISACs)

As an active member of the National Council of Information Sharing and Analysis Centers, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) announces the 2010 Critical Infrastructure Protection (CIP) Congress, 30 November to 2 December, at the Gaylord Resort & Convention Center, Washington, DC. The theme this year is “Manage Risk with Resilience.”

The goal of this year’s Congress is to provide CIP practitioners and concerned personnel (e.g., emergency responders) with solutions, best practices, and information to resist, respond, and reconstitute operations in the face of future threats. The event will feature plenary as well as several breakout sessions in various tracks centered on disciplines such as physical security, cyber security, resilience, and information sharing.

A detailed brochure with session descriptions is available at the conference [website](#).

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