



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

**INFOGRAM 39-09**

**October 1, 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](mailto:emr-isac@dhs.gov).*

### Emergency Services Sector Information Sharing

According to the FBI, the three foiled terror plots announced last week now make 26 publicly known treacherous schemes that have been disrupted by law enforcement since 11 September 2001. The failed plans “demonstrate just how far information sharing has come since 9/11, but also demonstrate that the threat of terrorism has not diminished.”

After reviewing a [29 September memorandum](#) by the Heritage Foundation regarding this recent success of information sharing, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) appreciates the importance of more information sharing throughout the Emergency Services Sector (ESS). While state and local fusion centers have certainly helped increase the passage and availability of information, the Heritage Foundation asserts that “more needs to be done to continue and expand the free flow of information.”

Increasing the expeditious movement of critical infrastructure protection, resilience, threat, and vulnerability information from the Department of Homeland Security (DHS) to ESS leaders, owners, and operators is the paramount EMR-ISAC mission. Nevertheless, there are hundreds of emergency departments and agencies that are not registered and subscribed with the EMR-ISAC to receive free sensitive and non-sensitive information.

Emergency organizations not participating in EMR-ISAC information sharing services may not be receiving consequential DHS information (For Official Use Only—FOUO) that could make a difference in their plans and operations before, during, and after a disaster strikes. (Note that there is a vetting/validating process to receive FOUO information). Therefore, to obtain a no-cost registration and subscription, send a request to [emr-isac@dhs.gov](mailto:emr-isac@dhs.gov) with all pertinent physical and electronic contact information. Questions can be answered by calling 301-447-1325.

### Communication and Public Health Emergencies

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) reviewed the “[Communication and Public Health Emergencies: A Guide for Law Enforcement](#),” (PDF, 1.4 Mb) created by the Police Executive Research Forum (PERF), with support from the U.S. Department of Justice.

This Guide identifies the considerations that law enforcement executives should address in their public health communications plans, regarding internal communications (i.e., those that remain within the agency) as well as external communications (i.e., those that go to other agencies or the public). When examining the PERF document, the EMR-ISAC learned that much of the content is equally applicable to the chief officers of the fire and emergency medical services.

[PERF](#) is a national membership organization of progressive police executives from the largest city, county and state law enforcement agencies. It is dedicated to improving policing and advancing professionalism through research and involvement in public policy debate.

## VBIED Update

National and international media sources have frequently reported about Vehicle Borne Improvised Explosive Devices (VBIEDs). For the benefit of Emergency Services Sector departments and agencies, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) reviewed the article “[Car Bombs: First Responder Concerns](#)” by [Officer.com](#), and summarized its contents regarding the use of passenger cars, delivery trucks, parked and moving vehicles as VBIEDs.

Vehicles are used to transport and detonate bombs because of the following capabilities:

- Conceal large amounts of explosives.
- Deploy in an easy and mobile manner.
- Provide an internal power-supply, switches, combustible material, and fragmentation.
- Attract little attention when moving or parked and unattended.
- Detonation can be accomplished remotely or by a timer.

The following are indicators when a VBIED may be present:

- Grease or dirt marks around compartment areas may indicate vehicle has undergone modifications.
- Weight distribution is not normal—engine or trunk area is too heavy or suspension is weighted down.
- Unusual chemical or gaseous type odor is present in or around the vehicle.
- Unknown leaking substances are visible in or around the out of view compartments.

If you suspect a VBIED, the following guidelines may be helpful according to the reviewed article:

- Clear—Leave the immediate area.
- Cordon—Establish a safe evacuation distance based on the [Bureau of Alcohol Tobacco and Firearms Explosives Standards](#).
- Control—Use binoculars from a safe distance to maintain visual surveillance of the vehicle.
- Call—Your local bomb squad.

More information regarding VBIEDs can be found at the [Homeland Security Knowledgebase](#).

## National Cyber Security Awareness Month

October is the 8<sup>th</sup> annual National Cyber Security Awareness Month (NCSAM), with the theme of “Our Shared Responsibility.” The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) verified that the Department of Homeland Security (DHS), the National Cyber-Security Alliance (NCSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are the primary drivers of NCSAM, and coordinate to promote the importance of cyber security as a shared responsibility.

According to the [NCSAM web page](#), our economy and much of the everyday infrastructure we rely on uses the web. The NCSA alleges that no individual, business, or government entity is solely responsible for cyber security. “Everyone has a role and needs to share the responsibility to secure their part of cyber space and the networks they use. Everyone needs to understand how their individual actions have a collective impact on cyber security.”

Electronic data networks are intimately linked to practically all elements of daily life in the 21<sup>st</sup> century, including critical infrastructure and key resources. NCSAM proponents maintain that growing reliance on networked operations and wireless data systems increases the potential for exploitation of gaps in electronic defenses.

NCSAM shares the following tips, which can be applied to protect emergency departments and agencies:

- Ensure that all computers have updated security software (anti-spyware, anti-virus, and firewall), web browsers, and operating systems.
- Set policy requiring employees to use long, complex passwords that they change at least every 60 days.
- Include or update cybersecurity practices in employee handbooks and insert policies regarding the use of mobile devices and laptops when offsite.
- Create a recovery or restoration plan in case you suffer a data loss.
- Make it policy to turn computers off at night and other down times.
- Delete unused and old data.
- Remain current on trends in cybersecurity and emerging threats.

The EMR-ISAC noted that additional information on how to protect your agency is available at [www.staysafeonline.org](http://www.staysafeonline.org) or [www.onguardonline.gov](http://www.onguardonline.gov). Cyber crime reports are accepted at [www.ic3.gov](http://www.ic3.gov).

## **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](mailto:nicc@dhs.gov)
- 2) Your local FBI office - Web: [www.fbi.gov/contact/fo/fo.htm](http://www.fbi.gov/contact/fo/fo.htm)
- 3) EMR-ISAC - Voice: 301-447-1325, E-Mail: [emr-isac@dhs.gov](mailto:emr-isac@dhs.gov), fax: 301-447- 1034,  
Web: [www.usfa.dhs.gov/emr-isac](http://www.usfa.dhs.gov/emr-isac), Mail: E-108, 16825 South Seton Avenue, Emmitsburg, MD 21727