



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

INFOGRAM 32-11

August 11, 2011

***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.*

Cyber Attacks Target Emergency Services

(Source: US-CERT)

With increasing frequency, criminals, terrorists, spies, and hackers are manipulating cyber technology including systems, applications, and devices to further their illicit objectives. According to the cyber specialists at the [U.S. Computer Emergency Readiness Team](#) (US-CERT), Internet technology has emerged as the preferred medium for hacker attacks and iniquitous communications to connect cohorts, plan activities, acquire supplies, and manage logistics.

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) gleaned from sources such as threatpost.com that hacker collectives claimed to have compromised the servers of 70 law enforcement websites across the southern and central United States. [The Associated Press](#) reported that one of the hacker groups alleges it has stolen 10 gigabytes of data, including emails, personal details, home addresses, and other information from local law enforcement bodies. (See the [Government Technology](#) article for more information regarding this hacking event.)

Unfortunately, with this level of information out in the public, those exposed by the leak are at grave risk of physical and emotional harm, identity theft, or massive compromise of online accounts. In a statement posted online, the groups said they feel no sympathy for the police officers and their informants, who they accused of “using and abusing our personal information, spying on us, arresting us, beating us, and thinking that they can get away with oppressing us in secrecy.”

Exploitation of existing vulnerabilities within Emergency Services Sector cyber systems can degrade essential capabilities such as computer-aided dispatching. This is a harsh reality for first responder organizations because computers and networks have become an integral internal infrastructure that cannot be interrupted or destroyed without jeopardizing continuity of emergency response operations.

US-CERT recommends any emergency organizations using networked technology should accept responsibility for securing their part of cyberspace by taking cyber risks seriously and using the safeguards available at [US-CERT](#), [OnGuardOnline](#), and the [National Cyber Security Alliance](#).

Civil Unrest Preparations

(Sources: firechief.com and fireengineering.com)

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) noted the incidents of unrest that recently occurred in [Wisconsin](#) and [Philadelphia](#). According to an article on page 48 of the July issue of [Fire Chief](#), such events raise the potential for involvement by fire and Emergency Medical Services (EMS) personnel in response operations for civil unrest.

With so much emphasis on preparations for natural disasters, accidental calamities, and terrorism, several fire and EMS departments may not have included civil unrest, disobedience or mass rioting in their training and all-hazards preparedness activities. Additionally, some emergency departments may not have conducted pre-planning to ensure standards and mandates are met during these situations.

To educate fire and EMS personnel about how to approach incidents of civil disorder or rioting, the [Firefighters Support Foundation](#) developed the [Fire/EMS Response to Civil Unrest Training Program](#). The 40-minute video and accompanying 46-slide PowerPoint presentation are available as a free download for training in the classroom, in the field, or with other agencies. Personnel can view the video while using the PowerPoint file as their hard copy notes, or they can use either resource independently.

EMS Workforce Agenda for the Future

(Source: NHTSA)

[The Emergency Medical Services Workforce for the Future](#) (PDF, 3.2 Mb), released by the National Highway Traffic Safety Administration (NHTSA), states Emergency Medical Services (EMS) personnel serve on the front lines of emergency medical care. It continues in the Executive Summary that the EMS system is vitally dependent on the ability of these workers to provide high quality emergent health care in dynamic and oftentimes dangerous circumstances.

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) acknowledges that the principal component of any EMS system is its workforce. Therefore, as seen in the Introduction of the document, “The ability of an EMS system to deliver high quality prehospital emergency care depends upon a qualified and capable workforce.”

The “EMS Workforce Agenda” envisions a future in which all EMS systems have a sufficient number of well educated, adequately prepared, and appropriately credentialed EMS staff who are valued, well compensated, healthy, and safe. The document identifies the following four components to developing an EMS workforce that will thrive and be a driving force for achieving integrated, community-based EMS systems: 1) personnel health, safety, and wellness; 2) education and certification; 3) data and research; and 4) workforce planning and development.

“The vision of the ‘EMS Workforce Agenda’ is ambitious but achievable with the continued collaboration of local, tribal, territorial, state, national, and federal EMS stakeholders.”

Assistance to Firefighters Grant

(Source: FEMA)

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) was notified that the [Assistance to Firefighters Grant](#) (AFG) open application period will run from 15 August to 9 September 2011. The primary goal of AFG is to provide funding for the essentials firefighters and first responders need to be safe and effective in the performance of duties.

Paid, volunteer, and combination fire departments and nonaffiliated EMS organizations from urban, suburban, and rural communities in the U.S. and its territories are eligible for AFG. This grant specifically supports firefighting and EMS equipment, personal protective equipment, fire and EMS vehicles, training programs, wellness and fitness programs, and modifications to facilities.

The [AFG Program Guidance and Application Kit](#) is now available for review. General AFG workshop information and the 2011 workshop schedule can be seen [here](#).

DISCLAIMER OF ENDORSEMENT

The EMR-ISAC does not endorse the organizations sponsoring linked websites, 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

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local FBI office and also the State or Major Urban Area Fusion Center. FBI phone numbers can be found online at <http://www.fbi.gov/contact/fo/fo.htm>. Fusion Center information can be seen at <http://www.dhs.gov/contact-fusion-centers>.

For information specifically affecting the *private sector* critical infrastructure contact the National Infrastructure Coordinating Center by phone at 202-282-9201, or by email at nicc@dhs.gov.

When available, each report submitted should include the date, time, location, type of activity, number of people, equipment used for the activity, name of submitting person and organization, and a designated point of contact.