



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

INFOGRAM 1-11

January 6, 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.*

Critical Infrastructure Resilience for 2011

(Source: National Infrastructure Advisory Council and EMR-ISAC)

During the past year, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) observed more Emergency Services Sector enhancements in the disciplines of critical infrastructure protection and resilience. Efforts continued in 2010 to reduce or mitigate the threats from natural disasters and terrorism at state, regional, and local levels with some guidance or assistance from the Department of Homeland Security Office of Infrastructure Protection (e.g., Protective Security Advisors).

Although no specific terrorist menace has been identified, every new day of 2011 brings new threat possibilities. America's enemies remain determined to attack particularly soft targets because of the perceived lack of security and the openness or exposure of personnel, physical assets, and communication/cyber systems (i.e., critical infrastructures). Furthermore, while flooding, tornadoes, and wildfires remain paramount concerns, no one can accurately forecast what "Mother Nature" will do this New Year.

Recognizing the possibility of future natural disasters and terrorist attacks, the leaders of the nation's emergency departments and agencies can resolve to proactively practice resilience measures for the critical infrastructures that cannot be protected as a result of scarce resources. The National Infrastructure Advisory Council defines infrastructure resilience as "the ability to reduce the magnitude and/or duration of disruptive events." Resilience measures should bolster an organization's capability to maintain mission essential tasks during a major catastrophe and restore normal operations very shortly after the event.

The staff of the EMR-ISAC extends best wishes for great success throughout 2011 with the selection and application of resilience measures appropriate for the survivability and continuity of each first responder organization and its community. Contact the EMR-ISAC at emr-isac@dhs.gov for more details regarding infrastructure resilience for man-made and natural calamities.

Cybersecurity in the Emergency Services Sector Webinar

(Source: Department of Homeland Security)

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) received notification that the Department of Homeland Security National Cyber Security Division will present the webinar "Cybersecurity in the Emergency Services Sector" at 1 p.m. on 20 January. To register for this opportunity, go to: https://connect.hsin.gov/cybersecurity_ess/event/registration.html.

The webinar will provide Emergency Services Sector (ESS) managers, practitioners, and first responders with an overview of the cyber vulnerabilities and threats facing the sector, with the purpose of heightening appreciation for the importance of strengthening cybersecurity in the field and at the workplace.

Additionally, it will review the types of cyber systems and infrastructure that emergency services organizations utilize, and address the threats and vulnerabilities to those cyber resources. Special emphasis will be placed on ESS unique challenges, and specific steps ESS personnel can take to mitigate cyber risk.

Questions about this webinar can be directed to essteam@hq.dhs.gov.

Protecting Emergency Personnel

(Source: Occupational Safety and Health Administration)

According to the Occupational Safety and Health Administration (OSHA), protecting Emergency Services Sector personnel is essential for assuring a successful response and recovery. "When large-scale disasters overwhelm state and local assets, the National Response Framework [Worker Safety and Health Support Annex](#) (PDF, 990 KB) can provide the technical assistance needed to help protect response and recovery workers."

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) noted that the annex describes the technical assistance resources, capabilities, and other support to ensure that response and recovery worker safety and health risks are anticipated, recognized, evaluated, communicated, and consistently controlled. It addresses the coordination and provision of technical assistance for worker safety and health management activities; it does not address public health and safety.

The annex is structured to provide technical assistance and support for response and recovery worker safety and health in the changing requirements of domestic incident management to include preparedness, prevention, response, and recovery actions. More information about available services can be seen at the [OSHA Quick Card](#) (PDF, 40 KB).

Private Sector Resources Catalog 2.0

(Source: Department of Homeland Security)

[Private Sector Resources Catalog 2.0](#) (PDF, 1.5 MB), released 15 November 2010 as the first update, facilitates access to the resources needed to participate in the homeland security enterprise and support the security of the United States. Targeted specifically towards private sector partners, the document collects the training, publications, guidance, alerts, newsletters, programs, and services available to the private sector across the Department of Homeland Security (DHS).

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) discerned that the catalog is organized by component and resource type and a comprehensive index is available to assist locating resources. Additionally, contact information across DHS can be found in Appendix A. The catalog is also available by [individual chapter](#) and may have information value to Emergency Services Sector departments and agencies.

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