



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

INFOGRAM 30-11

July 28, 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.*

Initiating a BC or COOP Program

(Source: DisasterResource.com)

Considering the ongoing potential for man-made and natural disasters, private and public organizations should take a simple approach to initiating a business continuity (BC) or continuity of operations (COOP) program, according to an [article](#) by Tim Bonno, an emergency management expert. An effective BC or COOP program enhances the ability for departments and agencies to maintain their essential operations across a broad spectrum of disasters.

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) acknowledges that a COOP program can bolster an organization's resilience, which is the capability to restore vital operations as soon as possible after the calamity. The Department of Homeland Security [Operational Framework for Resilience](#) (PDF, 806 Kb) indicates that resilience is the aggregate result of accomplishing resistance, absorption, and restoration during and after the catastrophe.

In his article, Mr. Bonno suggests five simple steps to BC that are also applicable for straight-forward COOP programs. The steps are summarized below for the consideration of the emergency services:

- Keep it simple and use common sense to identify what will have negative impact on operations and leverage opportunities to mitigate those things using an "all-hazards approach."
- Assemble a team of experts and decision makers for program planning and to notify in the event disaster strikes.
- Identify and document the critical organizational functions and an alternate site where they can be performed if necessary.
- Communicate with stakeholders and employees regarding plans and ensure everyone can use available communication technologies under pressure.
- Train and rehearse personnel so when an emergency occurs, they will know how to recover and reconstitute as quickly as possible.

See the FEMA [Continuity of Operations Overview](#) for more information.

Emergency Vehicle Security

(Source: FireRescue1.com)

As in past years, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) continues to receive information about stolen emergency vehicles that were unlocked with keys in the ignition. In a recent [incident](#), the stolen ambulance was left running outside a house fire "to keep it cool for anyone seeking medical care." At another [occurrence](#), the ambulance crew said they went inside the hospital for only a few minutes and left the keys in the ignition. When they came out the vehicle was gone.

Although the thefts are not an indication of a major problem among Emergency Services Sector (ESS) departments and agencies, it may still be a matter for concern and correction. The possibility exists that stolen emergency vehicles can be used to deceive emergency responders and security personnel for the purpose of committing criminal activity.

International experiences with stolen ambulances, fire apparatus, and police sedans have demonstrated that official vehicles typically draw less scrutiny and provide easier access to sensitive areas. This history supports the prudence of locking ambulances while rushing patients into hospital emergency rooms. Because of the frequency of vehicle theft within the United States, emergency departments and agencies can advocate locking the doors of every responder vehicle as well as securing the entrances and exits to the parking lots, stations, and garages where these automobiles are parked, stored, and repaired.

To reduce or eliminate emergency vehicle theft, ESS organizations can consider the appropriateness of a Standard Operating Procedures regarding the employment and security of their vehicles, including the requirement that all vehicles will be locked whenever and wherever unattended, with only few reasonable exceptions.

Third Needs Assessment of the U.S. Fire Service

(Source: National Fire Protection Association)

The National Fire Protection Association (NFPA) informed the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) regarding the release the third [Fire Service Needs Assessment](#) (PDF, 1.5 Mb).

The NFPA goal for this assessment was to identify major gaps in the needs of the U.S. fire service. To accomplish this goal, a comparison was made between what departments have and what they should have according to existing consensus standards, government regulations, and other nationally recognized guidance documents.

This third assessment follows two earlier surveys in 2001 and 2005, which were conducted under grants from the [U.S. Fire Administration](#). The executive summary includes not only a summary of the findings of the three needs assessment surveys, but also a summary of the implications of those findings for grant programs.

Technologies for Critical Incident Preparedness

(Source: DHS)

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) was notified by Department of Homeland Security (DHS) Office of Infrastructure Protection that the 2011 Technologies for Critical Incident Preparedness (TCIP) Conference & Expo will occur 30 August to 1 September, at the Gaylord National Hotel and Convention Center, National Harbor, Maryland.

This event, sponsored by the U.S. Departments of Defense, Justice, and Homeland Security, will bring together federal, state, local, and tribal practitioners; industry representatives; academic experts; and public safety associations. Their purpose is to share knowledge from the field about cutting-edge technologies and advances made over the past ten years that strengthen our nation's ability to prevent and respond to critical incidents.

More information about this event is available at the [TCIP website](#).

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.