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

INFOGRAM 50-11 December 22, 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@fema.dhs.gov.

SCBA Thermal Performance

(Source: U.S. Fire Administration)

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) was informed that the U.S. Fire Administration (USFA) and the National Institute of Standards and Technology (NIST) are studying the thermal performance of Self-Contained Breathing Apparatus (SCBA) face pieces. Increasing the protection to firefighters provided by this equipment, especially during incidents of high thermal exposure such as flashover, is the purpose of the joint research according to the USFA.

The initial phase of the study examined documented on-duty injuries and fatalities of firefighters due to thermal exposure of SCBA face pieces as well as conducting laboratory thermal testing of commercially available SCBA face pieces. Resulting from this research, NIST Technical Note 1724 titled "Fire Exposures of Firefighter Self-Contained Breathing Apparatus Facepiece Lenses" (PDF, 1.3 Mb) was released providing details about the testing.

"Thermally degraded and melted SCBA face pieces have been identified as a contributing factor in certain firefighter fatalities and injuries in the United States." Thus far, the experiments have demonstrated a range of realistic thermal exposures and environmental conditions, which can result in thermal degradation and even catastrophic failure of face pieces. However, "more experiments are needed to understand the thermal degradation and more definitively predict the conditions that are likely to cause a face piece lens failure."

Control Systems Security Program

(Source: DHS)

In its paper about the Control Systems Security Program (CSSP), the United States Computer Emergency Readiness Team (US-CERT) explained that critical infrastructures are dependent on information technology systems and computer networks for essential operations. To protect these cyber assets, including those of the Emergency Services Sector, Department of Homeland Security cybersecurity experts assisted by the National Institute of Standards and Technology developed the Cyber Security Evaluation Tool (CSET) (PDF, 168 Kb).

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) confirmed that CSET is a desktop software tool that guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems.

CSET has been designed for easy installation and use on a stand-alone laptop or workstation. It provides an excellent means for Emergency Service Sector departments and agencies to perform a self-assessment of the security posture of their system environment.

Blueprint for Cybersecurity

(Source: DHS)

The Department of Homeland Security (DHS) recently released the "Blueprint for a Secure Cyber Future" (PDF, 704 Kb). DHS designed this cybersecurity strategy to protect the critical systems and assets that are vital to the United States, and to foster stronger, more resilient information and communication technologies to enable government, business, and individuals to be safer online.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) noted that the Blueprint calls for a coordinated effort across the homeland security community to fortify our nation's critical information infrastructure and build a protected and more secure cyber ecosystem. Specific actions range from hardening critical networks and prosecuting cybercrime to raising public awareness and training a national cybersecurity workforce.

According to the DHS Fact Sheet, the Blueprint outlines an integrated and holistic approach to protecting our nation's cyberspace. "It is a map—a guide—to enable the homeland security community to leverage existing capabilities and promote technological advances that enable government, the private sector and the public to be safer online."

Active Shooter: What You Can Do

(Source: Emergency Management Institute)

Considering repeated active shooter incidents in the United States, the Emergency Management Institute (EMI) notified the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) regarding the availability of an interactive web-based course: (IS-907) Active Shooter: What You Can Do.

The course description explains that an active shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area. Typically, active shooter victims are selected at random and the events are unpredictable and evolve quickly.

Upon completing this course, participants should be able to describe the following: actions to take when confronted with an active shooter, actions to take to prevent and prepare for active shooter incidents, and how to manage the consequences of an active shooter event.

NOTE: There will be no INFOGRAM on December 29, 2011. The next INFOGRAM will be dated January 5, 2012. Happy and safe holidays from the staff of the EMR-ISAC!

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.