



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

INFOGRAM 24-09

June 18, 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.

Identity Theft Update

According to the Federal Trade Commission (FTC), identity theft occurs when someone uses your personally identifying information (e.g., name, social security number, credit card number) without your permission to commit fraud or other crimes. For example, "identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name." The FTC disclosed that most victims do not discover the theft until they review their credit report or a credit card statement and notice discrepancies.

To acquire an update regarding the status of identity theft in the United States, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) reviewed the [Government Accountability Office \(GAO\) study](#) released this week. The GAO and FTC found that as many as 10 million people become victims of identity theft each year. Although much publicity has been given to the matter of identity theft in recent years, both organizations confirmed that this crime is still a serious problem because of the continuing substantial harm it causes to increasing numbers of American citizens.

The EMR-ISAC learned that identity theft often leads to adverse consequences beyond financial loss. Confronted with inquiries about their reputation, wrongdoings, and no credit rating, many victims displayed tremendous annoyance, frustration, and embarrassment accompanied by diminished morale, emotional distress, clinical depression, and even loss of work. Some individuals have lost job opportunities, missed promotions, been refused loans, or been arrested for crimes they did not commit.

While steps have been taken at the federal, state, and local level to prevent identity theft, numerous vulnerabilities remain for public and private citizens. Recognizing that first responders can be victimized by this crime, Emergency Services Sector department and agencies can consult the [FTC](#) for suggestions to promote awareness and prevention.

Additional general information on this subject can be also obtained from the [FTC](#).

Wildland-Urban Interface Study

An article seen in the [June 16, 2009 NIST Tech Beat](#) discusses the National Institute of Standards and Technology (NIST) study that offers the first detailed look at the progress of a Wildland-Urban Interface (WUI) fire. "WUI fires are becoming more prevalent as housing developments push into former wilderness areas." Experience with these fires indicate that with the right wind conditions embers can be blown far ahead of the fire front starting spot fires hundreds of meters away.

The Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC) learned that the study revealed two-thirds of all the homes destroyed in the 2007 "Witch Fire" north of San Diego, CA, were ignited either directly or indirectly by embers. NIST researchers also verified that one-third of all structures within the fire perimeter were defended by first responders and/or homeowners. The "Witch Fire" resulted in injuries to 45 firefighters and two civilian deaths.

The NIST study confirmed that understanding WUI fire behavior is important to decrease risk to first responders and homeowners. Although firefighters are aware that embers ignite structures, little guidance is available to citizens to make their property more resistant to an ember attack. The researchers concluded that first responders frequently are put at risk because homeowners stay to protect their property.

This study is part of NIST's Reduced Risk of Fire Spread in Wildland-Urban Interface Communities research. For more information about this research refer to ["A Case Study of a Community Affected by the Witch and Guejito Fires."](#)

More information about WUI fire prevention and education methods can be obtained from the [National Interagency Fire Center](#) and the [U.S. Fire Administration](#).

Protecting the Protectors

In an article seen in [Government Security News](#), James Zeigler, a research associate at DuPont, Inc., acknowledged that to save lives and property, "first responders often put their own lives in jeopardy." He further asserted that "the global terrorist threat, coupled with the complexities of modern life, contribute a wide range of new dangers." To cope with this, the author recommended that emergency departments and agencies build a comprehensive plan that considers four elements: understanding the threat; understanding the priorities; understanding resources, roles, and responsibilities; and understanding equipment needs.

After examining Mr. Zeigler's four elements, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) appreciates how his "understandings" can contribute to reducing personnel injuries in the performance of duties. A quality critical infrastructure protection (CIP) plan will include these considerations when assessing the threats to and vulnerabilities of first responder organizations.

Identifying and reducing the vulnerabilities of internal critical infrastructures (i.e., personnel, physical assets, and communication/cyber systems) will bolster prevention and protection, and make the infrastructures more resilient to man-made and natural disasters. There are time-efficient, relatively simple, low-cost methods to reduce or eliminate threats and vulnerabilities. Some are limited more by imagination than by time and money.

Emergency Services Sector departments and agencies interested in a resource-restrained methodology for infrastructure protection and resilience can find useful recommendations in the [EMR-ISAC CIP Job Aid](#) and also in the free [CIP DVD](#) that can be ordered through the USFA Publications Center.

Revised NIPP Online Course

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) previously reported that Department of Homeland Security (DHS) Office of Infrastructure Protection released the [2009 National Infrastructure Protection Plan \(NIPP\)](#). The NIPP provides the unifying structure for the integration of existing and future critical infrastructure and key resources (CIKR). Part of the overall goal of the NIPP is to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.

The [Emergency Management Institute \(EMI\)](#) now offers a free on-line independent study course, [IS-860.a](#) National Infrastructure Protection Plan (NIPP), updated to align with the NIPP released in 2009. Course objectives include an explanation of the importance of protecting CIKR, identification of the relevant authorities and roles for CIKR protection efforts, and description of the underlying structure for the integration of CIKR protection efforts. Upon completion participants receive .2 CEUs.

EMI serves as the national focal point for the development of emergency management training to enhance the capabilities of federal, state, local, and tribal government officials, volunteer organizations, and the public and private sectors to minimize the impact of disasters on the American public. EMI instruction focuses on the four phases of emergency management: mitigation, preparedness, response, and recovery. EMI offers additional [online](#) and [residential](#) courses.

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: <http://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/subjects/emr-isac, Mail: J-247, 16825 South Seton Avenue, Emmitsburg, MD 21727