



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

INFOGRAM 25-09

June 25, 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.*

ESS: National Critical Infrastructure

In his address at a recent security summit, Deputy Assistant Secretary James Snyder of the Department of Homeland Security (DHS) Office of Infrastructure Protection discussed the impact of the [2009 National Infrastructure Protection Plan \(NIPP\)](http://www.hsd.org/hslog/?q=node/4704) (<http://www.hsd.org/hslog/?q=node/4704>) on the security of the nation's critical infrastructures and key resource (CIKR) sectors. Secretary Snyder explained that attacks on CIKR could significantly disrupt the functioning of governments and businesses in the United States, which are vital to preserving the nation's security, public health, safety, economic stability, and way of life.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) observed in this latest issue of the NIPP that departments and agencies of the Emergency Services Sector (ESS) remain among the prominently identified CIKR of the United States. Within the NIPP, the federal government again recognizes the important roles performed by ESS organizations that enable Americans to enjoy standards of living exceeding most countries of the world. DHS leaders acknowledged ESS essential duties such as assessing the vulnerability of CIKR sectors to a variety of dangers, and evaluating the physical integrity, unique operational challenges, and avenues of rescue and escape from different structures.

The EMR-ISAC substantiated that the Emergency Services Sector basically consists of law enforcement, fire, emergency medical, emergency management, and 9-1-1 organizations. In the context of the NIPP, Secretary Snyder said DHS efforts include strategies and actions that deter the threat, mitigate vulnerabilities, and minimize the consequences of a terrorist attack or natural disaster. The NIPP also encourages CIKR sectors (e.g., the emergency services) to initiate measures that enhance the protection and resiliency of the fundamental services upon which citizens depend.

Visit the [EMR-ISAC web page](http://www.usfa.dhs.gov/emr-isac) (<http://www.usfa.dhs.gov/emr-isac>) for more information about protecting the internal infrastructures of ESS departments and agencies.

Social Networking Concerns

During World War II, "loose lips sink ships" was the common admonition to keep small details about military movements and operations out of casual conversations among co-workers, friends, and relatives. In an article about the dark side of social networking seen in [Government Computer News](http://gcn.com/Articles/2009/06/18/DOD-on-dark-side-of-social-networking.aspx) (<http://gcn.com/Articles/2009/06/18/DOD-on-dark-side-of-social-networking.aspx>) David Carr wrote that social media web sites today thrive on loose lips, "making it even tougher to maintain operational security." The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) noted the author's assertion: "The problem is not so much people twittering away secrets as letting slip many smaller portions of information that adversaries can piece together."

According to the [Interagency Operations Security Support Staff \(IOSS\)](http://www.iooss.gov/) (<http://www.iooss.gov/>) operations security (OPSEC) is an analytical process to identify, control, and protect sensitive, but unclassified information for the purpose of denying opponents data they can synthesize to compromise an organization's operations, safety, and security. The primary emphasis of OPSEC is on identifying and protecting unclassified information about the planning and execution of sensitive activities.

Emergency Services Sector (ESS) leaders recognize their organizations have an abundance of unclassified information of high value to adversary intelligence collectors as well as local criminals. Through current and past research, the EMR-ISAC confirmed that criminal and terrorist elements desire sensitive but unclassified information regarding capabilities for various emergencies, command structure, incident command protocols, levels of competence, apparatus and equipment status, mutual aid agreements, emergency plans, standing operating procedures, response times, preferred routes, radio frequencies, call signs, etc. Therefore, the IOSS staff recommend practicing OPSEC by ensuring this type of critical information is not shared with the public through oral conversation, written communication, agency web sites, and the social networking sites such as Twitter, Facebook, LinkedIn, and Slashdot.

6 Minutes for Safety

The Federal Fire and Aviation Safety Team (FFAST) and the National Interagency Fire Center present "[6 Minutes for Safety](http://www.nifc.gov/sixminutes/dsp_sixminutes.php)" (http://www.nifc.gov/sixminutes/dsp_sixminutes.php). The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) noted that this is the first interagency safety initiative that, on a daily basis, addresses the high risk situations that historically have gotten first responders in trouble. According to this web site, "The fire community continuously works to find new ways to keep people safe on the fireline, and this initiative will have a tremendous positive impact."

As seen in a recent "[6 Minutes for Safety](http://www.nifc.gov/sixminutes/dsp_discussion.php?id=170)" tip (http://www.nifc.gov/sixminutes/dsp_discussion.php?id=170) firefighters need awareness of the potential hazards that have been summarized as follows by the EMR-ISAC:

- Hazardous materials used around the home may be dangerous from their flammability, explosion potential, and/or vapors.
- The increase of illicit activities in rural areas with items such as marijuana plants and meth labs.
- The potential for propane tanks, large (household size) or small (gas grill size) to explode.
- Utility lines located above and/or below ground that can be cut or damaged by tools or equipment.
- Below-ground structures, such as septic tanks, may not support the weight of apparatus.
- New construction materials may have comparatively low melting points and may "off-gas" extremely hazardous vapors.
- Plastic decking materials that resemble wood are becoming prevalent and may begin softening and losing structural strength at 180 degrees Fahrenheit.
- It is not uncommon for pets and livestock to be left behind. In some incidents residents resist evacuating. Firefighters should not put themselves at risk trying to protect animals or residents who will not evacuate.
- The limitation of roads and their capacity should be considered when preparing evacuation plans for residents and emergency personnel.

For more "[6 Minutes for Safety](http://www.nifc.gov/sixminutes)" tips (<http://www.nifc.gov/sixminutes>) click on the months seen to the right of the Calendar Display.

National Preparedness Month

According to the [Citizen Corps](http://www.citizencorps.gov) (<http://www.citizencorps.gov>) web site, their National Survey "[Personal Preparedness in America: the Citizen Corps National Survey June 2009](http://www.citizencorps.gov/pdf/Personal_Preparedness_In_America-Citizen_Corps_National_Survey.pdf)." (PDF, 2.38MB) (http://www.citizencorps.gov/pdf/Personal_Preparedness_In_America-Citizen_Corps_National_Survey.pdf) findings "have important implications for the development of more effective communication and outreach strategies to achieve greater levels of community preparedness, such as the relationship between risk perceptions and motivation to prepare, knowledge of emergency community preparedness procedures and resources, expectations of emergency responders, and how socio-economic factors affect preparedness."

The Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC) examined the findings of the survey that was done to evaluate the nation's progress on personal preparedness and to measure the public's knowledge, attitudes, and behaviors relative to preparing for a range of man-made and natural disasters. Survey questions addressed several critical areas in the field of disaster preparedness research including elements of personal preparedness such as stocked supplies, plans, knowledge of community protocols, and training; insights on barriers and motivators to preparedness; and social-behavior modeling on disaster preparedness.

An over-whelming 60 percent of respondents were unfamiliar about their local evacuation routes and 54 percent of respondents were unaware of the location of their local shelter. This uncertainty among community residents can potentially obstruct major response routes and seriously delay essential emergency services. Additionally, 57 percent of respondents expect to rely on their emergency personnel in the first 72 hours following a disaster.

The survey [summary sheet](#) (PDF, 64K) (http://www.citizencorps.gov/pdf/Personal_Preparedness_In_America-Citizen_Corps_National_Survey_SS.pdf) indicated that comprehension of respondents' attitudes and expectations can be used to achieve greater community resilience when preparing for disasters. The results of this study can also be applied to bolster the survivability, continuity, and response-ability of responder organizations.

On a related matter, the [National Preparedness Month](#) (NPM) (<http://www.ready.gov/america/npm09/index.html>) sponsored by FEMA's Ready Campaign and Citizen Corps, will be held in September to raise awareness and promote action surrounding emergency preparedness among citizens, businesses, and communities. This year it will focus on changing perceptions about emergency preparedness and helping Americans understand what it truly means to be ready.

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