



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

INFOGRAM 19-11

May 12, 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.*

HSIN Emergency Services Information Sharing

(Source: EMR-ISAC)

With the support of the Department of Homeland Security, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) recently established a community of interest (COI) on the Homeland Security Information Network (HSIN) portal to archive and share “For Official Use Only” (FOUO) information with vetted individuals occupying leadership positions within Emergency Services Sector (ESS) departments and agencies. The COI includes recent products, news feeds, and useful links divided into two sections: (1) federal, and (2) state, local, tribal, and territorial. The products in these two sections are categorized by border security, CBRNE, cyber security, terrorism, and other.

Fire service officers, police officers, emergency medical services supervisors, emergency managers, or 9-1-1 supervisors, serving in the United States or its territories, who are not vetted for access to the HSIN COI, should contact the EMR-ISAC to initiate the vetting process.

Although the EMR-ISAC will archive relevant sensitive information in the HSIN COI, this Center also disseminates by e-mail to vetted personnel the many DHS documents from the Office of Intelligence and Analysis or Office of Infrastructure Protection. This “push” service intends to expedite consequential information to those ESS decision makers having the “need to know.”

Individuals receiving e-mail from emr-isac@govdelivery.com with a link to an FOUO document should contact the EMR-ISAC for assistance if not able to open it.

It is important to understand that the no-cost FOUO information distributed by the EMR-ISAC may one day make a major difference in local emergency plans and operations. Therefore, it would be prudent for leaders in the emergency services to ensure they are properly vetted to receive the documents and conduct research in the HSIN COI.

The EMR-ISAC can be contacted at emr-isac@dhs.gov or at 301-447-1325.

Hoax White Powder Letters

(Sources: DHS and multiple media sites)

Although no specific information indicates plans by any group or individual to use the United States postal and shipping infrastructure to conduct or facilitate attacks, feigning the use of a biological weapon is a technique being used more frequently throughout the nation. These events are consuming more time of first responders, especially hazmat crews, according to the articles listed below.

See the following recent articles for examples of individuals who mail hoax white powder letters to draw attention to personal grievances, influence the behavior of their victims, disrupt normal government or commercial operations, etc.

- [Suspicious white substance forces evacuation.](#)
- [Letters with white powder sent to D.C. schools.](#)
- [Woman charged in White House anthrax hoax.](#)
- [Substance in courthouse letter harmless.](#)

When reviewing multiple media sources, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) verified that the majority of white powder found in threatening letters was determined to be non-hazardous. Nevertheless, the Department of Homeland Security "[Best Practices for Safe Mail Handling](#)" (PDF, 831 Kb) recommends that persons handling incoming mail and parcels should always exercise caution and be alert for the presence of hazardous substances.

For the benefit of Emergency Services Sector departments and agencies, suggested procedures for recognizing and responding to suspicious packages and mail can be seen at the [FEMA website](#), and also the Office of Compliance "[Safe Mail Handling Procedures](#)" (PDF, 696 Kb).

Disaster Preparedness Steps

(Source: Wall Street Technology)

In an article seen at [Wall Street Technology](#), Adam Montella, a homeland security and emergency management specialist, explained that protecting data is only part of a total preparedness solution for organizations. He reminded that it is essential to have a comprehensive plan in place to ensure organizational survivability and operational continuity. Additionally, he asserted that the planning process and training are the most important aspects of effective disaster recovery.

Mr. Montella advised organizations to use four steps when developing a continuity of operations (COOP) plan. Because they are applicable to the departments and agencies of the Emergency Services Sector, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) summarized the four steps as follows:

- Involve everyone in the planning process, including all stakeholders (e.g., government, private industry, community organizations).
- Consider organizational and community vulnerabilities to all hazards and plan for the worst-case scenario.
- Ensure all stakeholders know the details of the plan, train it, test it with periodic exercises, and continually improve it.
- Adjust the plan appropriately to the personal and family needs of organizational personnel during and after a disaster.

The author finished by sharing that COOP plans serve as the framework and general direction to follow, but do not take into account every scenario or contingency. "The plan does not tell you how to do your job, but rather how to do your job in a compressed timeframe, under stress, and possibly without all of your organization's resources in place."

See the [Continuity of Operations Overview](#) by the Federal Emergency Management Agency (FEMA) for more information.

Fraudulent Charitable Contributions

(Source: FBI)

Several States are recovering from disastrous tornadoes, while many States are currently dealing with catastrophic flooding. Some States have been affected by both tornadoes and flooding. Not surprisingly, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) learned that criminals are exploiting these tragedies for their own gain by sending fraudulent e-mails and creating phony websites designed to solicit contributions. Unfortunately, since late April, the [FBI](#) has received numerous complaints from citizens alleging fraudulent schemes.

The FBI reminds the public, including the many compassionate personnel of the Emergency Services Sector, to perform due diligence before giving contributions to anyone soliciting donations or individuals offering to provide assistance to those distressed by the disasters. Everyone must be watchful for solicitations from e-mails, websites, door-to-door collections, flyers, mailings, telephone calls, and other similar methods.

Before making a donation of any kind, consult the [FBI guidelines](#) to avoid being victimized.

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

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