



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

INFOGRAM 48-10

December 9, 2010

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.

First Responder Flu Vaccination

(Source: Centers for Disease Control and Prevention)

Recognizing the potential adverse effects on operational effectiveness caused by outpatient visits and hospitalizations, the [Centers for Disease Control and Prevention](#) (CDC) encourages Emergency Services Sector departments and agencies, as well as private sector businesses, to use their toolkit entitled: "[Make It Your Business to Fight the Flu](#)" (PDF, 2.7 MB).

When consulting with the CDC, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) ascertained that the Centers recommend a yearly flu vaccine as the first and most important step in protecting emergency personnel against a potentially serious sickness. This high-value, relatively low-cost prevention method can have the following benefits:

- Reduce absenteeism.
- Promote a healthier and more productive work force.
- Minimize possible disruption to emergency operations.

The EMR-ISAC noted that public health authorities are concerned about what they call "creeping complacency" among the public toward getting vaccinated for influenza. More information about this matter can be seen in a recent *Homeland Security Today* [article](#) about avoiding complacency.

Holiday Scams

(Source: FBI)

As the holidays approach, the Federal Bureau of Investigation (FBI) reminds the public to use caution when making online purchase. According to the [FBI National Press Release](#), cyber criminals continue to create ways to steal money and personal information. "If a deal looks too good to be true, it likely is." The Press Release offers several tips to avoid becoming a victim of cyber fraud.

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) confirmed that Emergency Services Sector personnel and their family members must be wary of e-mails or text messages indicating a problem or asking questions about financial accounts. It is a sad fact that criminals attempt to direct victims to click a link or call a number to update an account or correct a purported problem. The links may appear to lead a user to legitimate websites, but too often they are not, and any personal information shared on them could be compromised.

In another [FBI Press Release](#), the EMR-ISAC observed that the Bureau's Internet Crime Complaint Center provided additional suggestions to protect against cyber scams, particular those called "smishing" and "vishing."

Examining Success and Failures in Detecting U.S. Terrorist Plots

(Source: Institute for Homeland Security Solutions)

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) recently received the research brief, "[Building on Clues: Examining Successes and Failures in Detecting U.S. Terrorist Plots](#)" (PDF, 296 KB), published by the [Institute for Homeland Security Solutions](#) (IHSS). The Institute is a research consortium established to conduct applied research in the social and behavioral sciences to address a wide range of homeland security challenges. The consortium focuses on developing near-term solutions to practical, real world problems including an understanding and analysis of homeland security threats.

This particular research examined open-source material on 86 foiled and executed terrorist plots against U.S. targets from 1999 to 2009. The purpose of the study was to determine the types of information and activities that led to (or could have led to) their discovery and ultimate prevention. The findings provide law enforcement, homeland security officials, and policy makers with improved comprehension of the kinds of clues and methods that should be emphasized to more reliably prevent terrorist attacks.

The EMR-ISAC acknowledges the focus of the research is on the variety of activities terrorists engage in prior to attack, but also on the actions of law enforcement and the public at large that have proven most effective at thwarting plots.

National Fire Academy Resident Classes

(Source: U.S. Fire Administration)

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) was notified that the application period for the second semester of National Fire Academy resident classes closes Wednesday, 15 December. Second semester includes those classes scheduled from 1 April to 30 September 2011.

All information about courses, applications, and suggestions for successful completion of the application can be found at the following sites:

Course Catalog and schedules: www.usfa.dhs.gov/nfa/catalog/index.shtm.

Download Application: [FEMA Form 119-25-1, General Admissions Application \(formerly FEMA Form 75-5\)](#) (PDF, 629 KB). Use this application if your course code begins with the following letters: R, N, O, P, or T.

Tips to completing your application: [Eight Tips for Completing a Successful NFA Application](#) (PDF, 332 KB)

Completed applications for resident courses must be sent to the following address:

Office of Admissions, Building I, Room 216
National Emergency Training Center
16825 South Seton Avenue
Emmitsburg, MD 21727-8998
Applications may also be faxed to (301) 447-1441.

For more information, call the Admissions Office at (800) 238-3358, ext. 1035 or (301) 447-1035.

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: 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