



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

INFOGRAM 15-10

April 15, 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.*

2009 NIPP Regional Collaboration Emphasis

After reviewing the 2009 [National Infrastructure Protection Plan](#) (NIPP) (PDF, 4.5 MB) released late last year, the [Government Accountability Office](#) (GAO) discerned a significant change from the preceding version. In its [Highlights](#) (PDF, 61 KB), the GAO noted that the 2009 update places greater emphasis on regional collaboration through a consortium of stakeholders from multiple regional organizations.

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) confirmed that the revised NIPP encourages more cross-sector regional planning, coordination, and information sharing. At paragraph 4.1.3, the NIPP states regional organizations provide structures at the strategic and/or operational levels that can facilitate cross-sector critical infrastructure and key resources (CIKR) planning and protection program implementation. “They may also provide enhanced coordination among jurisdictions within a State where CIKR cross multiple jurisdictions and help sectors coordinate with multiple States that rely on a common set of CIKR.”

The EMR-ISAC acknowledges that “regionalization” may be a more desirable approach for local, county, and State leadership, emergency managers, and first responders to acquire scarce resources. Joining with other communities to develop regional plans and response packages of personnel and equipment can significantly improve the interoperability of mission-essential assets and systems. Additionally, pre-existing agreements and written plans that specify roles, payment, incident command, etc., should enhance thorough collaboration and synchronization among the numerous responding organizations within the region.

See sub-chapter 4.1 at page 12 of the [National Preparedness Guidelines](#) (PDF, 560 KB) for more information about regional collaboration.

Another Superbug Threat

According to an [article](#) in USA Today, clostridium difficile, a bacterium commonly known as “C.diff” has surpassed methicillin-resistant staphylococcus aureus (MRSA) as a serious threat to the nation’s medical facilities. It is spread by contact and can cause painful intestinal infections and in some cases death.

Considering the obvious threat to the Emergency Medical Services, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) consulted with the [Centers for Disease Control and Prevention](#) (CDC) and verified that “C.diff” spores are not easily eliminated with most conventional household cleaners or alcohol-based hand sanitizers. Medical research also substantiated that “C.diff” is resistant to some antibiotics.

“This superbug is especially difficult to stop because in addition to being a bacterium, it can exist in a dormant spore form, which can survive for weeks or months on hard surfaces, then begin multiplying when ingested.”

Common symptoms of “C.diff” include watery diarrhea 3 or more times a day lasting for more than 2 days and accompanied by mild abdominal cramping and tenderness. Serious cases of this bacterium are indicated by watery diarrhea 10 to 15 times a day, severe abdominal cramping, pains, fever, nausea, dehydration, loss of appetite, and weight loss.

The EMR-ISAC recommends MayoClinic.com for comprehensive information about clostridium difficile, particularly regarding symptoms, causes, risk factors, complications, tests and diagnosis, treatments, remedies, and prevention.

Spear Phishing: Dangerous Attack Vector

In a NextGov.com [cybersecurity report](#), Adam Ross wrote that spear phishing attacks have become increasingly sophisticated, tailored, professional, personal, and prevalent. The author further indicated that this malicious and criminally fraudulent action is among the most dangerous attack vectors that are exploiting organizations and their unsuspecting employees.

Instead of sending thousands of random e-mails hoping a few victims will bite, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) confirmed that spear phishers target select groups of people with something in common (e.g., firefighter, paramedic). The typical thread among recipients is that they work at the same organization, department, agency, bank, etc. The e-mails are ostensibly sent from organizations or individuals the potential victims would normally get e-mails from, making the messages even more deceptive. Consequently, the e-mails look authentic and offer urgent and legitimate-sounding explanations regarding why the recipient should click on a link inside the message. The link takes them to a fake but realistic-looking web site, where they are asked to provide user names, passwords, account numbers, access codes, PINs, and sometimes more.

A [paper](#) by the Federal Bureau of Investigation (FBI) recommends actions to avoid becoming a spear phishing victim. The EMR-ISAC listed the FBI suggestions as follows:

- Keep in mind that most organizations, departments, agencies, etc., do not request personal information via e-mail. If in doubt, give them a call, but do not use the phone number contained in the e-mail because that is usually phony as well.
- Use the phishing filter included in many of the latest web browsers or offered by them as a “plug-in.”
- Never follow a link to a secure site from an e-mail. Always enter the URL manually.
- Do not be fooled by the latest scams. Visit the [Internet Crime Complaint Center](#) (IC3) and [“LooksTooGoodToBeTrue”](#) web site for tips and information.

National Fire Academy Application Period

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) received information from the U.S. Fire Administration stating that the National Fire Academy (NFA) will begin accepting applications for the first semester FY2011 on 15 April. The application period will close on 15 June. The first semester includes classes that begin 1 October 2010 through 31 March 2011.

Interested individuals can examine the course schedule or conduct an advanced course search by using the following hyperlinks:

- [2010-2011 NFA Course Schedule](#)
- [NFA Advanced Course Search](#)

There are no tuition fees for NFA courses. All instruction and course materials are provided at no cost. Transportation expenses and lodging for students who represent career or volunteer fire departments, rescue squads, or State/local government attending on-campus courses are currently provided as part of funding under the student stipend reimbursement program.

Information regarding "[how to apply](#)" is available for downloading. The EMR-ISAC encourages applicants to review the "[8 Tips for Completing a Successful NFA Application](#)" (PDF, 328 KB) for helpful hints.

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